Information Management Support Center (IMCEN)
Information Systems Security (ISS)
Standard Operating Procedures (SOPs)

Prepared 14 October 1999 Last Updated 12 January 2000

Contents

1. INTRODUCTION

These *Standard Operating Procedures* are issued by the Headquarters, Department of the Army (HQDA) Information Management Support Center (IMCEN). They stipulate the Information Systems Security (ISS) responsibilities of appointed security officers and personnel who use automated information systems (AIS) within the HQDA Enterprise Network (HEN).

1.1 US Army Information Systems Security Program

This SOP implements the ISS Program (ISSP) as defined in Army Regulation (AR) 380-5, *Department of the Army Information Security Program*; AR 380-19, *Information Systems Security*; and AR 25-1, *The Army Information Resources Management Program*. It defines responsibilities of and contains instructions for Information Systems Security Officers (ISSOs), Organization ISSOs (OISSOs), System Administrators (SAs), division chiefs, supervisors, and individual automated information systems (AIS) users within the HEN and the IMCEN, which manages the HEN.

Every person assigned to HQDA IMCEN plays an indispensable role in the success of the ISSP. Without each individual's dedicated application of established security standards and procedures, the ISSP will have little impact on protecting our AIS and the information they process.

Address matters of ISS policy and procedures to Mr. Ronald L. Greenfield, Information Systems Security Manager, IMCEN, 695-7447. Users are invited to send comments and suggested improvements to this document to the Information Systems Security Officer (ATTN: William Dugger), 693-7070, Room 1D614, The Pentagon.

1.2 Purpose

The purpose of this SOP is to provide positive security against denial of services, disclosure of information, delay of information, and fraud concerning IMCEN automated Sensitive Defense Information. The objectives are to assign responsibilities and establish procedures to safeguard IMCEN automated information systems. Secure AIS can be achieved through aggressive management and user compliance to confront the risks, threats, and vulnerabilities associated with computer networks and information systems.

1.3 Scope and Applicability

(A) The ISSP as contained in AR 380-19 encompasses procedures from all other security programs as they pertain to automated information systems. The ISSP addresses the security of physical structures and environment, personnel reliability and security clearances, hardware security, data, and procedural security. Provisions of the ISSP are sufficient to ensure the effective safeguarding of classified and sensitive information.

(B) This SOP applies to all automated information systems operated within all agencies, divisions, branches, and offices associated with the HQDA Enterprise Network managed by IMCEN.

(C) **Automated Information Systems (AIS)**. IMCEN automated information systems include any assembly of computer hardware, software, or firmware configured to collect, create, communicate, compute, disseminate, process, store, or control data or information in an electronic form. AIS include stand-alone computers, small computers, word processors, multi-user computers, terminals, networks, and facsimiles.

(D) This SOP applies to all personnel assigned or attached to IMCEN. It is expected that all division personnel will be involved in the use of one or more types of AIS; therefore, each individual has the responsibility to understand and apply appropriate security procedures outlined in this SOP and in References 1 through 5 (see Appendix A).

1.4 Authority

(A) The security policies outlined are consistent with the framework established by existing laws, regulations, and guidelines, to include all References in Appendix A. Information Systems Security will be administered in accordance with these laws, regulations, and guidelines. In the event of a conflict between this SOP and other applicable regulations or directives the more stringent requirement will take precedence.

(B) Information System Security Officers (ISSOs), System Administrators (SAs), and Terminal Area Security Officers (TASOs) have the authority to make unannounced inspections to ensure compliance with this SOP. When observing violations, they will make on-the-spot corrections when possible.

1.5 General Requirements

The following applies to all personnel using AIS who are associated with the HQDA Enterprise Network.

(A) Each organization operating AIS within the HEN will delegate an Organization Information Security Officer (OISSO), to be appointed by either the head of the organization, his/her designated representative, or the Information Systems Security Manager (ISSM). Responsibilities of these positions are outlined in Section 1.6

(B) All local area networks require SAs.

(C) Any division within any of the field operating agencies may appoint a TASO.

(D) To ensure success of the ISSP, an ISSO, OISSO, and SA will be appointed for IMCEN by the ISSM. These positions will be delegated authority by prescribed directives and will be identified as ADP Sensitive, level II.

(E) **Responsibilities.** The protection of IMCEN automation assets, to include equipment and data, is the responsibility of all IMCEN employees, outside user personnel, and contractors who use or are associated with the operation of IMCEN automated information systems. Section 1.6 spells out the specific obligations and responsibilities of the various personnel comprising the IMCEN and HEN operations.

(F) **Security Briefing**. All incoming automation users of AIS within the HEN will read and be briefed on the contents of this SOP and will be required to sign the IMCEN Information Systems Security Inbriefing Form. A template for this form is contained in the IMCEN Certification and Accreditation packages (C&A Package 1 or C&A Package 2).

(G) Supervisors and personnel assigned automation security responsibilities will become familiar with AR 380-19, AR 380-5, and AR 25-1 (see Appendix A, References), as well as all locally prepared security SOPs.

(H) Classified information will not be processed or stored on automation equipment, except for the stand-alone systems that have been accredited for CS3 material. Privacy Act data and “FOR OFFICIAL USE ONLY” (FOUO) information shall be password-protected while stored on local drives. Password-protected means to store data in a private directory located on the server or to assign a password to individual files. Login passwords do not prevent access to non-password files that are stored on local drives. Off-site use of laptop computers will be in accordance with the accreditation of those systems.

(I) Labels affixed to magnetic media will be based on the highest level of information stored thereon. All magnetic media containing confidential information or higher will be labeled accordingly.

(J) Each individual assigned to IMCEN will be assigned a unique user identification and password. Passwords will be changed every 6 months or as required by AR 380-19. Control and password dissemination will be the responsibility of each agency’s SA.

(K) Unique applications developed by a user will be fully documented by that user in accordance with guidance supplied by the agency’s ISSO. The requirement for documentation of proprietary software is intended to ensure continuity.

(L) Hardware and software problems associated with automated information systems equipment will be reported to the agency’s SA or ISSO. This requirement is intended to provide early warning of equipment failure or software virus infection.

(M) Repair and maintenance of AIS data and hardware is handled through the IMCEN Help Desk. In the event the AIS fails, the Help Desk should be notified (693-4337) and requested to make the necessary repairs.

1.6 Responsibilities

All IMCEN employees, outside user personnel, and contractors who use or are associated with the operation of IMCEN automated information systems are responsible for the protection of IMCEN automation assets, to include equipment and data. The following subsections provide general SOPs and delineate specific duties and instructions for the following:

- Information System Security Managers (ISSM)
- Information Systems Security Officers (ISSO)
- Organization Information Systems Security Officer (OISSO)
- System Administrators (SAs)
- (OPTIONAL) Terminal Area Security Officers (TASOs)
- Division Chiefs and Supervisors
- Operators and End-Users

1.6.1 General

(A) The Information Systems Security Manager (ISSM) is the staff focal point for AIS security within IMCEN. ISSM duties, described in AR 380-19, include the management of AIS security matters affecting IMCEN and oversight of systems, activities, policies, training, and accreditation.

(B) The ISSM will appoint an ISSO to oversee AIS security matters. The ISSO will coordinate with the activities of the OISSOs and the SAs in the organization.

(C) SAs will be appointed by the agency for each AIS network for which they are proponents.

(D) (Optional) Terminal Area Security officers (TASOs) will be designated to supervise AIS security for each terminal or contiguous group of terminals not under the direct control of an ISSO or SA. This normally means within a room or a group of several adjacent rooms.

(E) Each Division Chief is responsible for ensuring that appointed personnel attend an IMCEN-sponsored Security Training class annually.

(F) Each Division will provide a copy of the Appointment Letter for each ISSO, OISSO, and SA to the IMCEN Information Systems Security Manager. The Appointment Letter must identify the area of responsibility by office name and room number.

(G) All Security Officers are responsible for ensuring that their systems are accredited, that they operate in accordance with the accreditation, and that the accreditation is properly maintained and updated.

(H) Each person who uses an AIS must be aware of and implement the necessary security safeguards for the AIS as contained in applicable Army regulations, this SOP, and any system-specific security guidelines issued by IMCEN AIS security officials. User questions regarding AIS security procedures or possible security problems should immediately be addressed to the appropriate security officer.

1.6.2 ISSMs are directed as follows:

(A) Oversee the execution of the ISS training and awareness program within the command or activity.

(B) Ensure that an ISSO is appointed for each separate AIS, group of AIS, or network, as necessary.

(C) Establish an AISSP that will provide protection for all information systems and ensures that all AIS and/or networks are accredited per AR 380-19.

(D) Periodically review the status of all AIS and networks to ascertain that changes have not occurred that affect security and negate the accreditation.

(E) Review threat and vulnerability assessments to enable the commander or manager to analyze properly the risks to the AIS information and determine appropriate measures to manage those risks effectively.

(F) Report security incidents and technical vulnerabilities per AR 380-19, AR 381-14, AR 380-5, and AR 381-12.

(G) Establish the scope of responsibilities for each ISSO using guidance from the ISSPM and applicable regulations.

1.6.3 ISSOs are directed as follows:

(A) Ensure that systems are operated and maintained according to AR 380-19 and governing SOPs.

(B) Ensure that managers, system administrators, and users have the appropriate security clearances, authorizations, and need-to-know.

(C) Work closely with their organization’s security manager.

(D) Prepare accreditation and reaccredidation documentation for organizational systems with the assistance of the SAs and TASOs.

(E) Include all personnel associated with AIS in system-specific and general awareness security training.

(F) Ensure that procedures, instructions, guidance, and SOPs concerning systems are prepared and distributed to all applicable managers, security officers, and system users.

(G) Randomly review operating system audit trails for unsuccessful login/on attempts and investigate discrepancies thoroughly.

(H) Report all security incidents and violations to the Information System Security Manager (ISSM) and his/her security manager.

(I) Direct their SA to disseminate User IDs and passwords to users as necessary.

(J) Coordinate with other ISSOs, security managers and SAs to determine levels of access for their agency personnel.

(K) Maintain accreditation documents for all systems for which they are responsible.

1.6.4 OISSOs are directed as follows:

(A) Ensure that individuals are appointed, as needed, for securing each terminal, workstation, computer, or associated group of computers that are not under the direct control of the ISSO.

(B) Ensure that managers, systems administrators, and users have the appropriate security clearances, authorizations, and need-to-know.

(C) Include all personnel associated with AIS in system-specific and general awareness security training.

(D) Report immediately to the ISSO any attempt to gain unauthorized disclosure and any loss of integrity or unavailability of system information.

(E) Evaluate and report to the ISSO the security impact of system changes, including interfaces with other AIS.

(F) Report security incidents and technical vulnerabilities to the ISSO.

(G) Prepare and provide all documentation in support of the preparation of the certification and accreditation of AIS.

(H) Maintain a current network or AIS certification or accreditation statement.

(I) Maintain access control records to ensure that only authorized personnel can gain access to the system.

1.6.5 System Administrators are directed as follows:

(A) Ensure that the networked system is properly operated and maintained.

(B) Ensure that that procedures, instructions, guidance, and SOPs concerning the networked system are prepared and distributed to those concerned.

(C) Establish procedures to control access and connectivity to the network.

(D) Ensure that system audit trails and system management reports are being used for internal security audits.

(E) Maintain a copy of the network accreditation documentation, and assist their ISSO in the preparation of accreditation documentation.

1.6.6 (Optional) TASOs are directed as follows:

(A) Implement security procedures and oversee the operation of terminal area systems.

(B) Maintain a list of individuals authorized to use automated information systems. The list will specify the level of classification users are permitted to operate systems.

(C) Ensure that automated information system users perform the duties outlined in AR 380-19 and applicable SOPs.

(D) Ensure that ISSOs/SAs are advised of changes in the location of equipment, modification of system hardware and/or software, and users having access to automated information systems.

(E) Oversee the enforcement of the following:

(1) Operators use only government supplied software.

(2) Operators make a copy of mission critical data at least once every two weeks.

(3) Operators use systems for official government business only.

(4) Operators do not process classified information on a system that is connected to a network. Operators process classified information only on systems that are disconnected from networks, and are accredited to process classified information.

(5) Operators do not leave PCs unattended while processing sensitive or classified information.

(6) Operators properly secure classified and sensitive data diskettes and printed output at the end of the day or when processing is complete.

(7) Operators do not eat or drink while using information systems.

(F) Inform all personnel that they are required to immediately report any actual or attempted access to any system with the intent to damage the system or commit fraud, extortion, theft, or misappropriation of funds, property, or services upon detection of the incident to their TASO, ISSO, or security manager.

(G) Identify and explain to users the existing regulatory requirements for security of remote terminal access to other systems and procedures governing remote terminal usage.

(H) Ensure that users understand the proper procedures for powering up/down their terminals, preventing disclosure of passwords when logging on/into a system and safeguarding a terminal connected to a host computer.

(I) Ensure that terminals are positioned to prevent disclosure of data by unauthorized viewing.

(J) Monitor terminal usage—type of output coming back to the terminals, access to terminals, etc. The TASO is required to be aware of what a terminal user is doing with a system.

(K) Ensure that display tubes are darkened or turned off at the end of the duty day. This will avoid burning of information onto the screen.

(L) Assist the ISSO/SA in providing system security.

(M) Report all practices dangerous to overall system security and all actual security violations to the ISSO/SA, as soon as recognized.

(N) The TASO will have ready access to accreditation documentation and be familiar with the level processed and the protective requirements associated with systems operated in the terminal area.

1.6.7 Division Chiefs and Supervisors are directed as follows:

(A) Maintain a hard copy of the IMCEN Information System Security Standard Operating Procedures (SOPs) and be thoroughly familiar with this SOP to support ISSP efforts within IMCEN.

(B) Contact the ISSO prior to moving any automation equipment within their division or office.

(C) Cooperate with the ISSO to ensure that all AIS within respective work areas are accredited as necessary.

(D) Assist the ISSO or OISSO to ensure compliance with ISSP policies and procedures.

1.6.8 Operators and End-Users are directed as follows:

(A) **Individual AIS Users – General**

All persons will comply with the following policies and procedures when using automation hardware, software, and products.

(1) Secure terminal areas at the close of each business day or when you are away from your computer for any extended period.

(2) Document any computer program or application created, designed, or modified by a user.

(3) NEVER share sign-on passwords with other personnel.

(4) Report hardware and software problems to the SA, ISSO, or OISSO assigned.

(5) Maintain cleanliness of automated equipment and the immediate areas.

(6) As soon as possible, report to your SA/ISSO or OISSO observations of security violations or any practices dangerous or threatening to system security.

(7) Ensure that classified information is not entered onto nonclassified systems.

(8) Ensure that information is treated and handled as required.

(9) Ensure that all monitors and printers are positioned to prevent unauthorized disclosure or casual viewing of Privacy Act information by unauthorized personnel.

(10) Ensure that the terminals and the main system are protected at all times by surge protectors.

(11) **Procedural Security:**

(a) Obtain an Information Systems Security briefing and understand security policy and procedures prior to operating an AIS and provide a hand receipt for all automation equipment, including software, in your individual workstation.

(b) Ensure that all AIS equipment is maintained with the utmost care. Operate equipment according to operation reference manuals and established security instructions.

(c) Ensure that all software applications run on your AIS have been approved and accredited. No personal copies of software will be brought into IMCEN or used on government-owned equipment without the ISSO’s approval. Honor software copyright restrictions. Make no unauthorized copies for office or personal use. Do not load software into other office computers unless authorized in licensing agreements. Do not borrow or remove software from workspaces.

(d) Ensure that no additional equipment is attached to a computer without the knowledge and permission of the ISSO. Additional equipment requires additional accreditation.

(e) Ensure that data files are saved to designated network home directories to ensure periodic backup copies.

(f) Safeguard assigned user passwords against compromise. Do not reveal your password to anyone else. If your password becomes compromised, report it immediately to the ISSO.

(g) Do not allow food or drink on or near automation equipment. This includes the table or desk on which the AIS are located.

(h) Ensure that your AIS is turned off at the end of the day, if it is not a “run 24-hour system.” Always log off the system after use or when leaving your office.

(i) Handle diskettes carefully to avoid damage. Ensure that there are no diskettes in the area that are without protective jackets. Never write on a diskette with pencil or pen; rather, write on labels and attach them to the diskettes.

(j) Report to the TASO or ISSO as soon as possible any security violation or practice that could be dangerous to security, damage equipment, or destroy information. Be especially watchful for and report to the ISSO immediately any irregular system operating characteristics. Your system could be infected with a virus.

(12) **Data Security:**

(a) All data being processed must be properly classified, marked, and handled in accordance with AR 380-5.

(b) All diskettes (classified or unclassified) must be labeled with the classification level, contents, and application program.

(c) Data output (paper products) must be marked at the top and bottom with the proper classification and required caveats prescribed by AR 380-5.

(d) Do not enter into an AIS classified information that exceeds the classification accreditation level of the AIS.

(e) “Need-to-know” applies to Information Systems Security. Do not allow any person outside your division or office to access your AIS unless authorized by your division chief and ISSO.

(B) **Operators Connected to Remote Computer Systems**

Operators using systems connected to a remote computer system are required to:

(1) Adhere to the security requirements for all remote terminals, individual passwords, and data transmitted to and from AIS.

(2) Comply with the provisions of the Privacy Act of 1974 when handling or processing privacy information.

(3) Comply with proper logon/in and logoff/out procedures.

(4) A remote terminal will be active only when an authorized terminal user is present and using the equipment. Any violation of this procedure is a breech of security. Each user must properly logoff/out the terminal prior to departing the area to ensure that access can only be gained by initiating proper logon/in procedures.

(5) Disclosure or transfer of User IDs and/or passwords from one user to another is prohibited.

(6) Terminal users will not transmit and/or extract classified data via unclassified remote terminals.

(C) Operators in a Stand-Alone Mode

System operators using systems that are operated in the stand-alone mode (not connected to a network) are directed as follows:

(1) Back up mission critical data at least once per week.

(2) Use the system for official government business only.

(3) Ensure that classified information is not entered on systems or equipment that do not have proper classified accreditation.

(4) Do not use unauthorized copies or install unauthorized copies of software on AIS. Operate software within the limits set forth in the software license agreement. “Bootleg” or illegally procured software and “shareware” are primary entry sources for computer viruses.

(5) Secure all unclassified sensitive data on diskettes and listings at the end of the duty day.

(6) Control the access to your system by powering down when unattended and using password functions of the menu programs.

(7) Discourage users from smoking, eating, or drinking while using a PC.

(D) Operators Connected to a Network

Operators using systems while connected to a network will:

(1) Protect their passwords at all times. Do not write them down or otherwise display them where unauthorized persons may observe them.

(2) Log off whenever you are away from their terminals for an extended period of time.

(3) Notify the SA, ISSO, or OISSO in the event of any security problem, breech, or suspicious activity.

(4) Do not load software onto a system without the prior approval of the ISSO.

(5) Personnel are not authorized to access the IMCEN wide-area network using remote node or remote control capabilities without the prior approval of the ISSM.

(6) Data processed, stored, and created on the network is official US Government property and will be protected at a minimum at the For Official Use Only level, following the need-to-know principle.

(7) Personnel will not process classified information on any system attached to a network. All classified processing will be accomplished while operating in a stand-alone mode only.

2. Computer Security

This section sets forth more detailed SOPs for the safeguarding of personnel, equipment, facilities, magnetic media, software, information, and data processing operations. It addresses the security requirements that specifically apply to the information—the *data*—produced and maintained in AIS. Included are the sensitivity designation of data processed, system criticality, the security processing modes authorized for use when processing classified or unclassified-sensitive data, systems classifications; and SOPs pertaining to WINS replication partners, backups, and Fortezza cards.

2.1 Sensitivity Designation

AIS sensitivity designation will be based on the highest classification or sensitivity of data processed as follows:

(A) **Classified Sensitive 1 (CS1)**. The AIS processes any Sensitive Compartmented Information (SCI) or Single Integrated Operational Plan Extremely Sensitive Information (SIOP-ESI) data.

(B) **Classified Sensitive 2 (CS2)**. The AIS processes any TOP SECRET data.

(C) **Classified Sensitive 3 (CS3)**. The AIS processes any SECRET or confidential data.

(D) **Unclassified Sensitive 1 (US1)**. The AIS processes UNCLASSIFIED data which requires protection from foreign intelligence services to ensure confidentiality and

(1) Involves intelligence activities

(2) Involves cryptologic activities related to national security

(3) Involves command and control of forces

(4) Is contained in systems that are an integral part of a weapon or weapons system

(5) Is contained in systems that are critical to the direct fulfillment of military intelligence missions

(E) **Unclassified Sensitive 2 (US2)**. The AIS processes UNCLASSIFIED data, which primarily must be protected to ensure its availability or integrity. This information:

(1) May also require protection from foreign intelligence services or other unauthorized personnel to ensure confidentiality. Examples include information dealing with logistics, medical care, personnel management, privacy act data, contractual data, and “for official use only” information, if not covered by US1.

(2) May require no protection to ensure data confidentiality. Examples include certain categories of financial data, routine administrative applications, and other data readily available through other sources.

(F) **Non-sensitive**. In rare cases AIS may be categorized as Non-sensitive provided they do not fall in any of the above categories. The Accreditation Authority must approve the Non-sensitive determination.

2.2 System Criticality

(A) Criticality is a measure of the importance of the system (including the data it processes) and the length of time that the system can be out of operation before loss of the system has an adverse impact on wartime operations. The level of criticality depends on the organization's ability to support wartime operations without the system. *Note: the criticality of a system is independent of the sensitivity level of the information processed*.

(B) In determining criticality, "loss" of the system refers not only to the availability of the system, but to the integrity of the system.

(C) Use the following categories to identify system criticality:

(1) **Group I—Mission Critical**. Loss of the system would cause immediate stoppage of direct mission support to wartime operations.

(2) **Group II—Mission Essential**. Loss of the system would cause eventual stoppage of direct mission support to wartime operations.

(3) **Group III—Mission Impaired**. Loss of the system would have a negative effect on (but would not stop) direct mission support to wartime operations.

(4) **Group IV—Non-Mission Essential**. Loss of the system would have no effect on direct mission support to wartime operations.

2.3 Mode of Operation

The security processing mode of operation is determined by the classification or sensitivity; formal categories of data processed; and the clearance, access approval, and need-to-know of the users. Formal categories of data are those for which a written approval must be issued before access (e.g., SCI, NATO, or Special Access Programs [SAPs]). AIS processing SAP information must also comply with confidential AR 380-381, Special Access Programs. All AIS will be accredited to operate in one of the following security processing modes:

(A) **Dedicated Security Mode**. All users of an AIS have the required personnel security clearance or authorization, formal access approval (if required), and need-to-know for all data processed by the AIS.

(B) **Systems High Security Mode**. All users of the AIS have the required personnel security clearance or authorization, but not necessarily the need-to-know for all data processed by the AIS. If the AIS processes formal categories of information all users must have formal access approval.

(C) **Partitioned Security Mode**. All users of the AIS have the required personnel security clearance or authorization, but not necessarily formal access approval and need-to-know for all information processed by the AIS.

(D) **Multilevel Security Mode**. Not all users of the AIS have the required personnel security clearance for all data processed.

2.4 Classification of System

(A) The AIS will be categorized based on the sensitivity of information that the system is authorized to process or store.

(B) The AIS that processes classified information will be designated by the highest classification, handling code, and category of information processed:

(1) Confidential

(2) Secret

(3) TS/SCI

(4) SIOP-ESI

(5) The AIS that processes unclassified information will be designated as SENSITIVE BUT UNCLASSIFIED (SBU).

2.5 Software Security

Another important part of automated system operation involves the use and protection of software. It is essential that we allow only authorized software onto the computer system, and then protect against unauthorized manipulation.

(A) The ISSO will provide guidance on who will install software.

(B) The ISSO, in conjunction with the IMCEN Configuration Control Committee (ICCC) has complete control over what programs are loaded into a system. The ISSO will ensure that all software is official—that it is procured by the Government or comes from an official Government source. All new software must be approved prior to installation.

(C) After procurement, the installer will test the software to ensure that it performs the functions for which it was procured, and that is contains no errors or detectable impurities.

(D) The installer will then introduce the software into the system and will maintain control over the master diskettes by storing them in a protected area.

2.6 WINS Replication Partners

(A) **Purpose and Scope.** This section establishes controls and procedures for WINS replication partners in the HQDA Enterprise Network (ARDA). Controls and procedures are necessary in order to ensure a reliable and stable WINS database. A stable database is needed to ensure reliable, consistent communication between workstations and servers on the Enterprise Network. A database with inaccurate entries will cause unpredictable and unreliable network communications.

(1) This SOP applies to HQDA activities replicating their WINS database with ARDA's WINS database.

(2) This SOP does not dictate or suggest how these activities should design or maintain their WINS database.

(3) This SOP is effective beginning 1 September 1997 and continues until superseded or made obsolete by the ARDA Network Management Office (IMCEN) or under agreement with supported activities.

(B) **Policy:**

(1) Beginning 1 September 1997, all activities replicating with ARDA's WINS database will inform the primary ARDA administrator of future replication with other WINS databases prior to establishing the replication.

(2) The primary ARDA administrator will then notify the other activities of the change.

(C) **Procedure for Establishing WINS Replication with ARDA:**

(1) A WINS replication request can come from within IMCEN or another HQDA activity. The request is to be forwarded to the primary ARDA administrator for approval.

(2) The primary ARDA administrator will evaluate the request. The following items will be reviewed:

(a) Identify resources in the Enterprise to which the requesting activity needs access.

(b) Determine whether it is possible for the requesting agency to use ARDA's WINS database as opposed to creating a replication relationship, thus reducing the number of WINS servers.

(c) Determine how many other WINS servers the activity replicates with. This number should be low or none at all. Identify the WINS servers that the requesting activity replicates with and list the owners within that database.

(d) Identify the NT domains that are contained in their database.

(e) Determine the stability and reliability of the activities' WINS server. A database with inaccurate records will only corrupt the ARDA's WINS database.

(3) If replication is necessary, an ARDA administrator will coordinate with the activity's WINS administrator to establish replication.

(4) The primary ARDA administrator will notify the other activities to expect additional IP addresses in their database due to the replication.

(5) The primary ARDA administrator will update the WINS as-built documentation to reflect the new replication relationship.

(D) **Procedures for Ensuring ARDA's WINS integrity:**

(1) The primary ARDA administrator will check the WINS Manager every 30 days to ensure that there are no unauthorized WINS owners in the database.

(2) The primary ARDA administrator will update the WINS As-Built documentation every 30 days or as needed.

2.7 Backups

(A) **Purpose and Scope.** This SOP defines the requirements and general guidelines for creating backups of network data. It also seeks to define a strategy for archiving backups. This section applies only to the HQDA Enterprise Network. Other backup systems may be mentioned due to their relationship with ARDA.

(B) **Responsibilities**:

(1) The primary ARDA administrator is responsible for ARDA's backup procedures and execution of backups. The primary ARDA administrator is also responsible for modifying this document as adjustments are made to the system.

(2) Other ARDA administrators are responsible for notifying the primary administrator if they modify any of the backup configurations.

(C) **Brief Definition:** The backup system consists of several different hardware and software platforms for performing a snapshot copy of network data and server configurations. Incorporated into this system are tape drives, disk copies, diskettes, and repair disks.

(D) **Design Goals:**

(1) Dependability. All critical systems will receive regular backups through an automated system. The frequency of these backups will be such that a significant amount of data will never be lost should a system failure occur.

(2) Reliability. The ARDA administrators are responsible for maintaining the reliability of the system. The primary administrator will review the procedures four times annually to verify system integrity.

(E) **Design Requirements:**

(1) The backups will be configured to minimize the time required to restore an entire system.

(2) The backup schedule will be automated and periodic backups initiated without user intervention.

(3) Backups will run through to completion without user intervention. A single backup job will require no more capacity than that which will fit on the storage device.

(4) The frequency of a complete backup will be no greater than one week.

(5) Each month a complete backup set will be set aside as an archive copy of the data that was backed up.

(6) Backup sets will not be collocated with the systems they backup. If the backup media is collocated, a fire and blast resistant container will be used as the storage location.

(7) Each backup set will be labeled appropriately as per the system that it is a backup for.

2.8 Fortezza Cards

(A) **Purpose and Scope.** This SOP defines the roles, responsibilities, and procedures for using, issuing, and protecting the Sensitive but Unclassified (SBU) Fortezza card for use with the Defense Message System (DMS) within IMCEN.

This SOP applies to anyone who receives his or her (SBU) Fortezza card through the IMCEN Organizational Registration Authority (ORA).

(B) **References.** (See References 15, 16, and 17, in Appendix A)

(C) **Brief Definition:** The Fortezza card is a personal computer card that uses approved algorithms and procedures to provide network related security services. A user may not access DMS unless that user possesses a Fortezza card; the PIN associated with that Fortezza card, and has the Fortezza software installed on their machine.

(D) **Responsibilities:**

(1) Organizational Registration Authority (ORA). Administrative authority that registers end-users of Fortezza cards with the Single Agency Manager (SAM) Certification Authority (CA). The ORA is responsible for gathering end-user registration information and forwarding it to the SAM CA, using the X.509 Certificate Request Form (see X.509 Certificate Request Form, and Instructions for Completing the X.509 Certificate Request Form). The Director of IMCEN, or whomever he delegates this authority to, will appoint the IMCEN primary ORA and any alternates on orders and will complete and forward the ORA Appointment Memorandum to the SAM (see Organizational Registration Authority (ORA) Appointment Memorandum). The ORA responsibilities include:

(a) Works with users to complete X.509 Certificate Request Form (Appendix C).

(b) Verifies individual’s identity and security clearance.

(c) Coordinates with CA to obtain a Distinguished Name (DN) for the user or organization.

(d) Reports suspected compromise of Fortezza cards.

(e) Provides information about Fortezza cards from the CA to the users.

(2) Fortezza Card User. Member of an organization who is designated by his supervisor to require use of DMS and as a result requires a Fortezza card. The user responsibilities include:

(a) Properly filling out the X.509 Certificate Request Form.

(b) Using and safeguarding the Fortezza card IAW this SOP.

(3) Supervisor. The supervisor responsibilities include:

(a) Identifying users who require use of DMS.

(b) Verifying information on the X.509 Certificate Request Form.

(c) Training users on this SOP and ensuring they follow the provisions contained within the SOP.

(E) **Physical Control:**

(1) Fortezza cards must be protected much like credit cards to limit the possibility of loss, unauthorized use, substitution, tampering, or breakage. Programmed cards

may not be left in the open and must be secured. Fortezza cards must be secured when carried by the user away from their work location (vacation, conference, etc.).

(2) Fortezza PINs associated with Fortezza SBU cards should be memorized. PINs will not be written on the Fortezza cards, or maintained in the vicinity of the Fortezza workstation. Users may record PINs, but the Pin's must be stored securely and separately from the associated card.

(3) Workstations containing Fortezza software, including laptops, must be protected in a manner that will minimize the possibility of loss, tampering, or unauthorized use.

(4) Fortezza cards associated with a particular user must not be shared. The recipient's ability to determine the authenticity of messages is assured only if senders use the card assigned to them.

(5) The user must remove the Fortezza card from the workstation if they leave the immediate area.

(6) No one except the person who is identified as the user on the X.509 certificate request form may possess both the Fortezza card and the PIN at the same time.

(F) **Fortezza Reportable Events.** The following events must be reported to the ORA, supervisor, or IMCEN security personnel within 24 hours after the event. The POC outside of normal duty hours is the Pentagon Telecommunications Center (PTSC) at (703) 695-2291/92.

(1) Card Loss – Temporary or permanent loss of a Fortezza card.

(2) Pin Compromise – Actual or suspected compromise of the PIN associated with a Fortezza card.

(3) Card Misuse – Actual or suspected misuse of a Fortezza card.

(4) Software Modification - Unauthorized modification of Fortezza software installed on a workstation.

(5) Card tampering – Actual or suspected tampering with a Fortezza card.

(6) Duplicate Card Abuse – Unauthorized use of an authorized duplicate Fortezza card.

(7) Unreported Personal Data Changes – User failure to notify the Certificate Authority (CA) or ORA of card data changes such as departure or job change.

(8) Card or PIN not Received – Failure of a user to receive a requested Fortezza card from the programming CA/ORA in a reasonable time.

(9) Premature Card Disabling – Detection that a user's card is disabled prior to his making the ten unsuccessful consecutive attempts to unlock it.

(G) **Reportable Event Details.** When reporting a reportable event, users must include the following data:

(1) User's name, Distinguished Name, internal chip serial number, and organization.

(2) Identity of all certificates on the affected card, and the identity of the programming CA.

(3) Complete circumstances surrounding the incident, including the physical security situation.

(4) Identity and job assignments of any other personnel involved in the incident.

(5) User's assessment of whether the affected card, PIN, and/or Fortezza software was compromised.

(H) **Procedures for Obtaining/Returning Fortezza Card/DMS:**

(1) Supervisor designates user who requires DMS and the Fortezza card and software to accomplish their duties.

(2) User completes the X.509 Certificate Request Form, has the form signed by their supervisor and gives the form to the ORA.

(3) ORA reviews and signs the form then forwards the form to the CA.

(4) The user will receive the Fortezza card and PIN either through hand delivery, or through the mail. If it is received through the mail the PIN and Fortezza card will be mailed separately to different addresses.

(5) The user will sign and return to the CA an Advisory Statement and Receipt. By doing this, the user verifies and accepts receipt of the card, PIN, and certificates listed on the Certificate Report provided with the card. When the user signs the advisory statement, they are verifying they understand the responsibilities associated with possession of a Fortezza card.

(6) The user will maintain a record of all certificates on their cards and the programming CA. Users will store the Certificate report provided with each card.

(7) The ORA will receive a copy of the Advisory Statement and receipt from the PTSC. The ORA will use the information from this report to monitor Fortezza cards in the organization and to perform any required inventories.

(8) Users will turn in the Fortezza card when they depart the organization or when the card is no longer required. The user may turn in the card through hand delivery, or

may ship the card according to the provisions of the Single Agency Manager (SAM) Certification Guide (Reference 4).

(9) The Supervisor will ensure that the user returns the Fortezza card and that this information is reported to the ORA. The ORA will assist the user in returning the Fortezza card when required.

2.9 Physical Security

2.9.1 General Safeguards

(A) All visitors to the computer operational area will be challenged and escorted as necessary to preclude unauthorized access to unclassified sensitive information.

(B) The AIS will be protected at all times with a surge protector.

(C) Uninterruptible Power Supply (UPS) will be interconnected with the fileserver in the LAN.

(D) Good housekeeping will be practiced at all times. Excess paper products and flammables will not be stored in the AIS operational area. The AIS will be kept free of dust and other contaminants to the extent possible.

(E) Smoking, eating, or drinking of any beverage in the immediate vicinity of the AIS is prohibited.

(F) Procedures for access to rooms containing classified systems are outlined in the IMCEN Classified AIS Accreditation Guidelines.

(G) Keys to the facility will be maintained in a key depository; access to which will be controlled IAW AR 380-19. DA Form 5513R will be used for accounting and inventory purposes.

(H) AIS will not be left unattended while any user is logged into the system.

(I) All personnel will be instructed on handling telephonic bomb threats IAW building location(s) occupancy emergency plan(s).

(J) Close of business day checks will be annotated on SF 701, Activity Security Checklist.

2.9.2 Magnetic Media Protection

Magnetic storage media is an integral part of most computer configurations. Additional precautions are necessary whenever information is stored on totally removable magnetic media.

(A) Magnetic media, particularly diskettes or “floppies,” will not be bent, squeezed, poked, clipped, or touched on the oxide surface. They are sensitive to heat, cold, magnetism (from any source), and physical abuse. Using the common sense approach when handling magnetic media will afford them the best protection.

(B) Each set of magnetic media will be labeled to reflect the originator, information about what is contained on the media, and periods (dates) covered on the media.

(C) The SF 71O (Unclassified) security classification label for magnetic media is not required in a totally unclassified environment. (See AR 380-19 for information on handling magnetic media in a classified environment.)

(D) Physical storage of the media must be secure. Magnetic media must be protected against environmental and physical elements and against unauthorized access, based on the sensitivity of the information.

2.9.3 Laptop Computers

Laptop computers can very easily be concealed in a brief case, paper bag, under a jacket, or among other unsuspecting items of equipment. If a laptop is misappropriated, the perpetrator has successfully stolen a valuable piece of Government equipment, and the potentially sensitive information contained therein. For these reasons, additional precautions must be taken to protect laptops from theft or unauthorized use.

(A) Extracts of the SOPs dealing with the safeguarding of laptops will accompany each laptop when removed for off-site processing. This will afford the user immediate guidance in the event a question arises regarding the safeguarding of the equipment or information processed while away from the home station. Other considerations are as follows:

(1) Information processing. Laptop and portable computers, regardless of location, must comply with the same requirements as stand-alone computers for processing classified or unclassified-sensitive information.

(2) Laptop and portable computers must be accredited to process classified or unclassified-sensitive information. The accreditation must address all aspects of security and must specifically indicate the approved processing sites. If the accreditation is for processing while on temporary duty a copy of the accreditation document must be with the computer at all times.

(3) In no case will classified processing be authorized at any location other than US Government or US Contractor approved locations. If the accreditation document so provides, classified processing may be done on laptop or portable computers if it occurs in normal work areas otherwise acceptable for the storage, preparation, or discussion of classified material.

(4) Physical protection: Laptop computers are high-value items; users must safeguard them at all times:

(a) In the absence of an approved security container or locked office in a Government facility, the laptop must be locked inside a secure storage compartment at all times that it is not in possession of the user.

(b) Any media or other material produced by the computer must be handled and secured IAW AR 380-5.

(c) While traveling in aircraft, carry the laptop onboard and maintain physical possession of it at all times.

(B) The ISSO has the responsibility to ensure that each user of laptops is aware of his or her responsibilities whenever these computers are removed for off-site processing. The aforementioned precautions will be addressed during training sessions. As previously mentioned, an extracted copy of the portion of the SOP pertinent to the safeguarding of laptop computers should be kept with each laptop.

2.9.4 Remote Devices and Off-Site Processing

(A) Remote terminal devices must be secured according to the mode of operation and information that the remote terminal is authorized to access. Approval to process Government information at locations other than at the normal work site takes effect upon authentication of the IMCEN approving official, the individual, and the HQDA IMCEN Information Manager (IMCEN LOI #2-98).

(B) Remotely accessed computer systems and file servers must possess features to positively identify users and authenticate their identification before processing.

(C) Classified defense information will not be processed at the off-site work location, regardless of ownership, without prior specific written approval from the Agency Security Manager and the Designated Accreditation Authority.

(D) Government-related work processed on a PC, regardless of whether the PC is privately or Government-owned, is the property of the U.S. Government.

2.9.5 Fire Protection

(A) Fire prevention procedures will be in accordance with existing regulations and SOPs.

(B) A fire extinguisher will be available in each room housing AIS equipment.

(C) All persons assigned to the AIS will receive instructions on the use of the fire extinguishers.

2.10 Procedural Security

Procedural security measures involve a minimum of financial expenditure while producing a high level of security. The following covers ARDA Administrator account controls and procedures, user account management, user password controls and procedures, and auditing procedures.

2.10.1 ARDA Administrator Account Controls and Procedures

(A) **Purpose.** This section establishes controls and procedures for administrative access to the HQDA Enterprise Network currently known as ARDA. The source of these policies is HQDA ARDA SOP 98-09 (15 July 1998), which supersedes HQDA ARDA SOP 97-1, Administrator Password Controls and Procedures. This SOP is effective beginning 15 July 1998 and continues until superseded or made obsolete by the ARDA Network Management Office (IMCEN).

(B) **Scope.**

(1) Individuals having these levels of access have extensive, and even complete, access and permissions to the entire HQDA Enterprise Network. Access to these permissions must be closely monitored in order to avoid unauthorized access and possible negligence.

(2) This section does not apply to administrator passwords on other networked systems that are not a member of the HQDA Enterprise.

(3) Neither does this SOP apply to user accounts not having administrator privileges. User account passwords are addressed in Sections 2.10.2 and 2.10.3 and in Section V of AR 380-19.

(C) **Policies:**

(1) The use of the ARDA Administrator account is granted to authorized personnel who need it to fulfill their duties. Authorized personnel include individuals employed by the Systems Management Branch in IMCEN who are responsible for systems within the Enterprise Network.

(2) The Administrator account will be used only when absolutely necessary; administrative tasks will otherwise be performed with the user’s own (named) network account.

(3) Only the Chief, Systems Management Branch, and the designated government ARDA Administrator will grant use of the Administrator account.

(4) Personnel entrusted with the password to the Administrator account will under no circumstances share it with anyone else. An ARDA administrator will change the administrator password on a regular basis for security purposes.

(D) **Procedures for Password Distribution:**

(1) The password will be printed on an ARDA Administrator Password Signature Sheet. Individuals requiring the password will sign the sheet acknowledging that they will not disclose the password to unauthorized personnel.

(2) The administrator who changes the password is responsible for (a) notifying the primary ARDA administrator of the change and (b) ensuring that the new password is distributed as described. Once the sheet has all the required signatures, it will be given to the primary ARDA administrator for safekeeping.

(E) **Physical Security.** The primary ARDA administrator will safeguard the ARDA Administrator Password Signature Sheet in an appropriate secured device. Only ARDA management personnel shall have access to that device.

(F) **Procedure for Password Changes:**

(1) The administrator password will be changed every 60 days or when an individual who is employed in the Network Management Office terminates his position, which ever occurs first.

(2) The primary ARDA administrator is responsible for changing the password once it reaches its maximum password age.

(3) If the Network Management Office no longer employs an individual, the Network Management Office supervisor must notify an ARDA administrator. The administrator must change the password as soon as possible then distribute the password as defined below.

(G) **Password Content:**

(1) The password's minimum length is 9 characters.

(2) The password should not be a word found in the dictionary.

(3) The password can be generated at the discretion of an ARDA administrator.

(H) Other Accounts Having Administrator Access

(1) Authorized personnel may be granted NT Administrator rights by including their NT accounts in the Administrator group. Authorized personnel include individuals employed by the Systems Management Branch in IMCEN who are responsible for systems within the Enterprise Network.

(2) This access will only be granted to those authorized personnel needing it to fulfill their duties. Only the Chief, Systems Management Branch, and the designated government ARDA Administrator will grant administrator rights.

(3) Personnel granted administrative rights will under no circumstances grant administrator, server operator, or account operator rights to any other user without approval by the Chief, Systems Management Branch, or the designated government ARDA Administrator.

(I) Account and Server Operator Privileges

(1) Authorized personnel in ARDA may be granted rights as Account Operator and Server Operator. Authorized personnel include individuals employed by IMCEN who are responsible for account and server maintenance within the Enterprise Network.

(2) These privileges may also be extended to designated personnel of other HQDA Enterprise organizations whose membership exceeds 100 people. Personnel given these privileges are obligated to follow the published operating procedures for the ARDA domain when exercising those privileges.

(3) As with the other administrative accounts, this may be done only with the explicit approval of the Chief, Systems Management Branch, or the designated government ARDA Administrator.

(J) General Provisions

(1) Users with administrative access of any kind are especially cautioned to be careful in the use of their accounts. Passwords will not be shared with other personnel. Passwords will not be so simplistic that they might be easily guessed.

(2) Workstations or servers will not be left logged in and unattended; when leaving a machine, users will log out or lock the workstation.

2.10.2 User Account Management

(A) **Purpose and Scope.** This section establishes controls and procedures for creating and deleting users' accounts on the HQDA networks for which IMCEN is responsible.

(1) It applies only to HQDA local area networks (LANs) for which IMCEN is responsible for managing.

(2) This SOP does not apply to HQDA LANs that have their own Information Management Office performing their network management.

(3) This SOP is effective beginning 1 September 1997 and continues until superseded or made obsolete by the ARDA Network Management Office (IMCEN).

(B) **Policy**:

(1) Beginning 1 September 1997, all user account management requests will be sent via the Exchange mail system.

(2) A User Properties Change Request form will be filled out electronically via e-mail. The HQDA administrators will review the form and take appropriate action.

(C) Procedure for Establishing or Modifying a User Account:

(1) Anyone (an information management officer [IMO], Help Desk technician, or an end user) who needs a user account to be created or modified will fill out a User Properties Change Request form. This is an electronic form found in the Exchange mail system.

(2) The User Properties Change Request form requires the following information (any additional information can be entered in the Processing Instructions field):

(a) Requested action (add, modify, or delete account)

(b) Full name of the end user (including middle initial and rank)

(c) Agency and Office Symbol

(d) Room Number and Location

(e) Phone Number and Fax Number

(3) Once the User Properties Change Request form is completed and sent, the HQDA administrators will automatically receive a notification via e-mail. They will open the User Properties Change Request form in the User Properties Change Request folder and review the information. The requesting activity’s point-of-contact may be notified to verify the information.

(4) If the user account belongs to a NetWare LAN or a non-Enterprise network, the account will be created or modified in accordance with that LAN’s standards.

(5) If the user account is for the HQDA Enterprise Network, the HQDA administrator will forward the request to the Enterprise User Account Manager. The account manager will create or modify the user account in accordance with the Enterprise standards.

(6) Once the request is complete, the HQDA administrator or the Enterprise User Account Manager will modify the User Properties Change Request form to reflect that the action is complete.

(7) The Help Desk will monitor the User Properties Change Request folder for completed actions. If the request requires further action, the Help Desk will initiate a work request.

(D) Procedures for Deleting a User Account:

(1) Anyone (an information management officer (IMO), Help Desk technician, or an end user) who needs a user account to be deleted will fill out a User Properties

Change Request form. This is an electronic form found in the Exchange mail system.

(2) The User Properties Change Request form requires the following information (any additional information can be entered in the Processing Instructions field):

(a) Select the Delete Account option

(b) Full name of the end user (including middle initial and rank)

(c) Agency and Office Symbol

(d) Room Number and Location

(e) Phone Number and Fax Number

(3) Once the User Properties Change Request form is completed and sent, the HQDA administrators will automatically receive a notification via e-mail. They will open the User Properties Change Request form in the User Properties Change Request folder and review the information. The requesting activity's point-of-contact may be notified to verify the information.

(4) If the user account belongs to a NetWare LAN or a non-Enterprise network, the account will be deleted. The user's home directory and e-mail account will also be deleted.

(5) If the user account is for the HQDA Enterprise Network, the HQDA administrator will forward the request to the Enterprise User Account Manager. The account manager will be deleted. The user's home directory and e-mail account will also be deleted.

(6) Once the request is complete, the HQDA administrator or the Enterprise User Account Manager will modify the User Properties Change Request form to reflect that the action is complete.

(7) The Help Desk will monitor the User Properties Change Request folder for completed actions. If the request requires further action, the Help Desk will initiate a work request.

2.10.3 User Password Controls and Procedures

(A) **Purpose and Scope.** This section establishes controls and procedures for individual password accounts on ARDA, HQDA Enterprise Network.

(1) This SOP applies to the password assigned to all individual accounts on the ARDA NT domain.

(2) This SOP is effective beginning 1 July 1997 and continues until superseded or made obsolete by the ARDA Network management Office (IMCEN).

(B) **Policy:**

(1) All passwords provided to and used by individuals are critical to the security of the system. All persons having access to passwords must be carefully instructed on password sensitivity and the meticulous care with which such critical information must be protected and the individual’s personal responsibility and obligation to cooperate.

(2) Each authorized user must log on the system with a valid user ID and password. If compromise of the password is suspected, the user will immediately notify the TASO/ISSO.

(3) Passwords must be created by the user and not be a word that can be found in the standard dictionary, contain a minimum of 9 characters in length, include at least one special character or number, and must contain letters that are a mixture of upper and lower case.

(C) **Procedures for Password Changes:**

(1) The user’s access to an activity in the system will be controlled and open to scrutiny.

(2) The TASO will brief all users about their responsibility regarding password security. Users will be instructed not to reveal their passwords and to use caution regarding their surrounding to prevent onlookers from compromising their passwords.

(3) Users must change their passwords once every 180 days.

2.10.4 Auditing

(A) **Purpose and Scope.** This SOP establishes controls and procedures for auditing the HQDA networks for which IMCEN is responsible.

(1) This SOP applies only to the unclassified HQDA local area networks (LANs) for which IMCEN is responsible for managing.

(2) This SOP does not apply to HQDA LANs that have their own Information Management Office performing their own network management.

(3) This SOP is effective March 27, 1998 and continues until superseded or made obsolete by the ARDA Network Management Office.

(B) Policy:

(1) ARDA Audit Policies. The ARDA Audit Policy is set to the following events:

Event	Success	Failure
Logon and Logoff		X
File and Object Access	X	X
Use of User Rights	X	X
User and Group Management	X	
Security Policy Changes	X	X
Restart, Shutdown, and System	X	X
Process Tracking		X

(2) Auditing Event Logs. Upon receipt of an administrative alert, an administrator will check the event log of the server generating the alert.

(3) Administrative Alerts. Administrative alerts are event messages generated by Windows NT. These alerts warn about problems in areas such as security and access, users sessions, directory replication, printing, and server shutdown because of loss of power. Windows NT predetermines the selection of the events that trigger administrative alerts. Alert examples are a disk is near capacity or too many logon violations have occurred.

The domain controllers for ARDA will be configured to send administrative alerts to administrators. The Server and Alerter services must be stopped and started when specifying who is to receive administrative alerts. After receiving an administrative alert, the administrator will further investigate the cause of the alert.

2.11 Personnel Security

Most of the requirements for this phase of the Automated Information System Security Plan (AISSP) are accomplished by the personnel security support element of an organization. For this reason, investigative requirements and the screening and evaluation process are not addressed. Although each personnel security support office will be handling most personnel security needs, designation of position sensitivity levels remains a responsibility of the supervisor. Other required aspects of the program are as follows:

2.11.1 General Policy

(A) When individuals who will be associated with the operation of automation equipment are assigned to an organization, they must receive an initial information systems security briefing regarding their assigned responsibilities and be given a clear definition of their specific duties in relation to the organizational mission. In addition, they must read these SOPs—or, at a minimum, those sections that apply to their assignment—and must sign a Security Inbriefing Statement (see C&A Package 1 or C&A Package 2 for a copy of this statement).

(B) Employees will be continually updated (throughout the year, but not less than annually) regarding their information systems security responsibilities. A portion of this requirement can be satisfied through incorporation of an information systems security segment into the annual topics of continued concern to all automated information system users. Included in these sessions will be the identification, reporting, and precautions taken against system intrusion and contamination.

(C) AR 380-5, 1-320.1 Foreign national employee is a person who is not a citizen or national of, or immigrant alien to, the United States. Each foreign national who requires access to unclassified information to perform their duties must have a favorable National Agency Check or host country equivalent per 380-67, 2-17b in order to access AIS.

2.11.2 Security Training and Awareness.

All individuals appointed as ISSM, ISSO, and System Administrator must complete an AIS Security course of instruction commensurate with the duties assigned to them. All other personnel who manage, design, develop, maintain, or operate AIS will undergo a training and awareness program consisting of the following topics:

(A) An initial security training and awareness briefing for AIS managers and users to include:

(1) Risk associated with the system to reduce the threat from malicious software

(2) Password security, information accessibility

(3) Responsibilities and accountability associated with system security

(4) Network certification/accreditation

(5) Emergency and disaster plans

(6) Physical and environmental considerations that are necessary to protect the system

(B) Periodic security training and awareness to include:

(1) Self-paced, Web-based presentations/briefings

(2) Security education bulletins

(3) Training films

(4) Electronic security tips

3. Processing Information

IMCEN AIS are used to process unclassified information. IMCEN AIS will not be used to process classified information.

3.1 Virus Protection

(A) The use of antiviral products provides the greatest protective countermeasure for virus protection, detection, and treatment. IMCEN AIS will not be used to process information unless IMCEN approved antiviral software has been installed.

(B) If a virus is discovered on an IMCEN AIS, the user is authorized to use the current antivirus software to disinfect. This must be done before sending any files out or inserting any disks.

(C) For those not technically trained, the IMCEN User Help Desk must be notified so that designated technical personnel can verify the virus, determine the origin, if possible, and treat appropriately.

(D) The user will file a virus report via email, using the format located in the public folders, to VirusReports@hqda.army.mil.

(E) The ISSO and ISSM must be notified immediately upon detection of any new viruses.

3.2 Processing US2 Data on a Non-Networked AIS

The following pertains to stand-alone, non-networked AIS:

(A) Prior to processing US2 information, physical access controls commensurate with the level of processing will be established.

(B) The AIS must be accredited to process US2 data.

(C) All users of the AIS must possess the appropriate authorization and need-to-know for the data handled by the AIS.

(D) Connections to external hosts, modems, networks, PCs, or other communications links are permitted. Users must follow the security procedures provided by the host system. Permission to access other systems is granted by the host system. Ensure that the ISSO, SA, or TASO has approved information transmitted.

(E) The video display terminal and printer must be positioned, relocated, or other safeguards applied, such as drawing blinds or window shades, to preclude viewing from corridors, open hallway, doors, windows, or by passers-by or other unauthorized personnel.

(F) If the system or printer is to be accessed by users without the appropriate authorization and need-to-know, all sensitive media and removable printer ribbons must be properly secured.

(G) Workstations are not to be left on and unattended unless password enabled screensavers are activated or system lock feature is used.

3.3 Processing US2 Data on Networks

(A) The network and all connected AIS must be accredited to process information at the appropriate level.

(B) All IMCEN networks operate in the systems high security mode wherein all users of the network possess the required personnel security clearance or authorization, but not necessarily the need-to-know, for all data handled by the network.

(C) All terminals linked to IMCEN networks will require a user ID and Password. Terminals will be locked-out after three incorrect log-on attempts during a 24-hour period. To be unlocked the user must notify the System Administrator.

(D) Passwords and user identification (user ID) to access the network will initially be assigned by the appropriate System Administrator (SA) after signing the IMCEN Information Systems Security Inbriefing Form.

(E) Users must change their passwords every 180 days. Passwords will be at least eight characters long, include at least one special character or number, and must contain letters that are a mixture of upper and lower case. Passwords will not be a word that is found in standard dictionaries.

(F) Passwords will be handled, stored, and protected at the level of the most sensitive data contained in the system. If possible, passwords should be committed to memory. A password must never be disclosed to anyone.

(G) Users may permit appropriately cleared personnel access to their individual data elements only after determining a legitimate need-to-know.

(H) Connections to external hosts, modems, networks, PCs, or other communications links are permitted. Users must follow the security procedures provided by the host system. Permission to access other systems is granted by the host system. Ensure that the ISSO, SA, or TASO has approved the information transmitted.

(I) Users must never transfer data to another user unless the clearance and legitimate need-to-know have been verified.

(J) The video display terminal and printer must be positioned, relocated, or other safeguards applied, such as drawing blinds or window shades, to preclude viewing from corridors, open hallway, doors, windows, or by passers-by or other unauthorized personnel.

(K) If the system or printer is to be accessed by users without the appropriate authorization and need-to-know, all sensitive media and removable printer ribbons must be properly secured.

(L) Users must log-off when leaving the network or the terminal. An unoccupied terminal must never be left logged-on to the network. When possible, network software will provide for a time-out/auto log-off feature.

3.4 Notification Banner

(A) Welcome or Greeting Banners will not be used on IMCEN networks. It can be difficult to prosecute anyone for unauthorized use of Federal Government computers with Welcome/Greeting Banners.

(B) The following notice will appear on all IMCEN networks:

> THIS IS A DOD COMPUTER SYSTEM. BEFORE PROCESSING CLASSIFIED INFORMATION, CHECK THE SECURITY ACCREDITATION LEVEL OF THIS SYSTEM. DO NOT PROCESS, STORE, OR TRANSMIT INFORMATION CLASSIFIED ABOVE THE ACCREDITATION LEVEL OF THIS COMPUTER SYSTEM. THIS COMPUTER SYSTEM, INCLUDING ALL RELATED EQUIPMENT, NETWORKS AND NETWORK DEVICES (INCLUDES INTERNET ACCESS) ARE PROVIDED ONLY FOR AUTHORIZED U.S. GOVERNMENT USE. DOD COMPUTER SYSTEMS MAY BE MONITORED FOR ALL LAWFUL PURPOSES, INCLUDING TO ENSURE THAT THEIR USE IS AUTHORIZED, FOR MANAGEMENT OF THE SYSTEM, TO FACILITATE PROTECTION AGAINST UNAUTHORIZED ACCESS, AND TO VERIFY SECURITY PROCEDURES, SURVIVABILITY, AND OPERATIONAL SECURITY. MONITORING INCLUDES, BUT IS NOT LIMITED TO, ACTIVE ATTACKS BY AUTHORIZED DOD ENTITIES TO TEST OR VERIFY THE SECURITY OF THIS SYSTEM. DURING MONITORING, INFORMATION MAY BE EXAMINED, RECORDED, COPIED, AND USED FOR AUTHORIZED PURPOSES. ALL INFORMATION INCLUDING PERSONAL INFORMATION, PLACED ON OR SENT OVER THIS SYSTEM MAY BE MONITORED. USE OF THIS DOD COMPUTER SYSTEM, AUTHORIZED OR UNAUTHORIZED, CONSTITUTES CONSENT TO MONITORING. UNAUTHORIZED USE OF THIS DOD COMPUTER SYSTEM MAY SUBJECT YOU TO CRIMINAL PROSECUTION. EVIDENCE OF UNAUTHORIZED USE COLLECTED DURING MONITORING MAY BE USED FOR ADMINISTRATIVE, CRIMINAL OR OTHER ADVERSE ACTION. USE OF THIS SYSTEM CONSTITUTES CONSENT TO MONITORING FOR ALL LAWFUL PURPOSES.

4. HQDA E-MAIL SITE POLICIES AND GUIDELINES

4.1 Purpose and Scope

This SOP implements new operational guidance on the establishment of HQDA Exchange Network policies. The source for these guidelines is Letter of Instruction #1-99 (see Reference 11).

This operational guidance provides HQDA enterprise-level e-mail site policy and configuration guidance that applies to all HQDA organizations per Army CIO guidance (Reference 20).

4.2 Exchange, General Administration

(A) All mail policies will be kept in a public folder for general access. This will facilitate the incorporation of new or revised policies.

(B) The organization name is ORGANIZATION, and the site name is HQDA.

(C) Naming conventions for the Defense Message System (DMS) software applications and for the server/host on which these applications are loaded are being developed by the Defense Information Systems Agency (DISA). Once these documents are coordinated throughout the DOD, this LOI will be reevaluated to ensure compliance.

(D) Administrators for organizations that have their own Exchange server, but are in the HQDA site will have control over their server as Server Operators in the ARDA NT domain. However, connections to other sites and systems should be cleared with HQDA site administrators before execution.

(E) Those organizations having their own Exchange server will be totally responsible for the add/change/delete of user accounts on their server, although HQDA site administrators can act as a backup.

(F) Connections in the site (SMTP, MS Mail, Site, etc.) will only be set up and run by the site administrators.

(G) Each organization in the HQDA site will have its own recipients container.

(H) For each organization that joins the HQDA site a high-level folder will be created with that organization’s name. The administrators of the various organizations will have the ability to add/change/delete/set access rights on public folders for their organization within their specific high-level folder.

(I) Replication of public folders should be coordinated with the HQDA site administrators as replication has implications for network bandwidth. Similarly, the establishment of affinities to public folders should also be coordinated with HQDA site administrators.

(J) All forms in the site should be registered with HQDA site administrators, but that is only for information exchange and to prevent needless duplication of form creation/programming.

(K) HQDA site administrators should be notified of planned outages of a HQDA server at least three days in advance. Every effort should be made to plan these outages outside of Monday through Friday, 7AM to 5PM.

(L) HQDA site-wide distribution lists should be coordinated through the HQDA site administrators. This will prevent unnecessary duplication of distribution lists.

4.3 Exchange, User Configuration

(A) User accounts are created with an alias name using the AMSME standard of: `lastname+firstinitial+middleinitial`, truncated as necessary to 15 characters (that is, the last name will be truncated to 13 characters).

Duplicate names on a system are resolved by the addition of a numeral, beginning with “2”. (Example: SmithJD2) Information on the fields in the user account, whether they are designated mandatory or not, and their content, is given under “Exchange User Account Fields” below.

(B) **SMTP Addresses:**

(1) The default SMTP reply address will be, per AMSME guidance, firstname.lastname@HQDA.Army.Mil.

(a) Duplicates will be resolved by the addition of a numeral, beginning with “2” to the last name (example: John.Smith@HQDA.Army.Mil)

(b) For users who have the legacy “5-1-1” address, that address will be retained as secondary address.

(2) If an organization has an existing SMTP gateway, that gateway address may also be included, though the gateway’s address is transferred to the Exchange site.

(3) The local administrator may within reason, add other SMTP aliases.

(a) For users on servers managed directly by the HQDA site administration team, mailbox storage is currently limited to 48 MB with a warning given between 30 and 38 MB. These levels must sometimes be adjusted to ensure that server’s Private Information Store does not grow beyond safe limits. Mailbox storage limits for servers managed by partner agencies are set by the local administrators, who are also responsible for monitoring the size of the server’s Private information Store.

(b) Personal folders should be kept in the user's home directory unless the primary workstation for the user is a notebook. In that case, it should be kept on the notebook.

(c) Any user giving "Send As" rights to another user should inform the HQDA site administrators.

(C) Exchange User Account Fields

Name	Use	Actual
First	M	Given name
Initials	M	Middle initial; if none, leave blank
Last	M	Last name
Display	M	(See "Display Name Format")
Alias	M	See above for format
Address	M	Building code or full mailing address
City, State, ZIP code, Country	O	Used if full mailing address is used in the Address field
Title	M	Military: rank; civilian: "Mr.," "Ms.," etc. No punctuation
Company	M	Your organization (e.g., ASA-FM, DISC4)
Department	R	Any division or group within the organization
Office	M	Room number
Assistant	O	Another person in your organization
Phone	M	Commercial phone, separated with hyphens
Phone/notes, Business		Linked to "Phone" on General tab
Business 2	M	DSN number
FAX	O	
Pager	O	

M = Mandatory **R** = Recommended **O** = Optional

4.4 Account Display Name Format

IMCEN and the Pentagon Single Agency Manager have agreed to follow the display name format which has been adopted by the SAM and which is basically the same as that in the draft convention being distributed by the Army Signal Command.

(A) General

(1) Display names will make use of the following four fields using data already stored in the user account:

(a) Last name

(b) First name and middle initial

(c) Title or rank (from Title field)

(d) Organization (from Company field)

(2) Display names may be updated by the local administrators, <u>or</u>, if local administrators prefer, done en masse by the Exchange Administrators.

(3) New accounts must have the display name entered according to the adopted convention.

(B) **Description of the Format.** Per AMSME guidance, the display name will consist of four fields:

Field 1 Last name

Field 2 First name and middle initial; generation qualifier may be included here, if desired

Field 3 Title – For civilians, Mr., Ms., Dr., etc., with no punctuation; for military, rank in the standard abbreviations (LTC, SSG, etc.).

Field 4 Organization name - this should be the highest level of the organization; all users in an Exchange container should use the same organization name.

(C) A comma and a space will separate the last and first names; all other fields will be separated by a single space. There will be no punctuation other than the single comma.

(D) **Examples**.

Public, John Q LTC DISC4

Burke, Miranda S Ms OCPA

Walters, William D SSG DCSPER

Smith, James H Jr. Mr. IMCEN (note generation qualifier)

Reynolds, Barbara R ASA-FM (note absence of title)

4.5 Organizational and Resource Accounts

(A) **Organizational** accounts are those that do not belong to a specific user, such as “Help Desk”. Resources are similar, but are used primarily for non-mail functions such as scheduling (for example, “ASA-FM Conference Room”). Display names for such accounts start with the organization’s container name, so they will be easily identified and sorted together in the global address list. For organizations whose container names may not be unique (for example, there are multiple “DCSPERs” throughout the army), the organizational acronym may be used instead (in DCSPERs case, DAPE).

(B) **Resource** accounts should be created in the organization’s subfolder of the Resources container. Organizational accounts may be placed in the organization’s recipients’ container.

(C) **Fields** will be filled as follows:

First Name The name of the account itself (for example, “Conference Room”)

Last Name The name of the organization (for example, “ASA-FM”)

Display Name The organization’s name followed by the resource name (that is, Last Name plus First Name, similar to how users’ display names are built; for example, “ASA-FM Conference Room”)

Company The organization name (same as Last Name)

Other The remaining fields may be filled in at the discretion of the administrator.

4.6 Distribution Lists

Distribution lists can be set up by local administrators to fit the needs of the organization. The following guidelines cover their configuration:

(A) All distribution lists should be created in the organization’s appropriate sub-container of the Distribution List container.

(B) Display names for distribution lists should start with the organization’s container name, so they will be easily identified and sorted together in the global address list. Like distribution lists, for organizations whose container names may not be unique, the organizational acronym may be used instead (for example, DAPE instead of DCSPER).

(C) Distribution lists should be “nested” as much as possible. That is, where all members of one group are also members in another group, the second list should contain the first distribution list as a member, instead of individual accounts being added to both. This is useful in organizational trees, where members are added to a branch distribution list, and then the branch distribution lists added to a divisional distribution list. This reduces the number of places where individual account names must be added or deleted.

4.7 SMTP Custom Recipients

Custom Recipients may be added to make SMTP addresses for users outside the Exchange organization available. Because this affects users throughout the Exchange organization "ORGANIZATION", the adding of such listings should always be coordinated with the HQDA Site administrators.

(D) Depending on the circumstances, custom recipients may be put in an organization's site sub-container (e.g., Recipients/CSA), a subcontainer to the subcontainer (e.g., Recipients/DISC4/SMTP), or another container altogether (e.g., Associated Mail Systems). HQDA Administrators will be responsible for how custom recipients are added into site folders.

(E) The display name format for custom recipients is identical to that for mailboxes.

(F) The required fields, unlike those for mailboxes, are only those required by Exchange and the display name:

Name	Use	Actual
First	M	Given name
Initials	M	Middle initial; if none, leave blank
Last	M	Last name
Display	M	(See "Display Name Format")
Alias	M	See above for format
Address	M	Building code or full mailing address
Title	M	Military: rank; civilian: "Mr.," "Ms.," etc. No punctuation
Company	M	Your organization (e.g., DCSPER, ASA-FM, DISC4)

M = Mandatory **R** = Recommended **O** = Optional

(G) All other fields are optional

5. Certification and Accreditation (C&A)

Certification is the technical evaluation that establishes the extent to which a particular computer system meets a pre-specified set of security requirements for use in a particular environment. The Certifying Official makes a recommendation for or against accreditation based on this evaluation.

Accreditation is a formal declaration by the Single Agency Manager (SAM) Designated Approving Authority (DAA) that an information system or network is approved to operate:

- In a particular security mode
- With a prescribed set of countermeasures
- Against a defined threat and with stated vulnerabilities and countermeasures
- Within a given operational concept and environment
- With stated interconnections to other information systems
- With an appropriate level of protection (level of risk) for which the DAA has formally assumed responsibility
- For a specified period of time

In approving a system for operation, the DAA formally accepts responsibility for the security of the system and declares that the system will provide an appropriate level of protection against compromise, destruction, or unauthorized modification of data when operated under the conditions stated in the accreditation.

Certification and accreditation of systems must be accomplished separately for each level of overall system classification. Systems accredited by SAM will fall into one of four categories: Unclassified/SBU; Confidential; Secret; or Top Secret**.**

5.1 Explanation of Requirements

(A) **All** DOD automated information systems (including networks and stand-alone computers) must be accredited **prior to being placed in service**.

(B) Agencies seeking accreditation must address a request for accreditation to the organization’s ISSM, who evaluates the request and forwards his/her recommendation to the DAA (see Section 5.2, C&A Documentation Requirements).

(C) **Reaccredidation:**

(1) A system must be reaccredited every three years, at a minimum. The Certifying Official should start the reaccredidation process at least three months prior to the end of the current accreditation. This will provide an overlap in the accreditations and help ensure that the accreditation of the system will not lapse for any period of time.

(2) Reaccredidation is also required as a result of significant changes to the system configuration, operation, or environment. Some examples of changes that would require reaccredidation:

(a) Increase in sensitivity level (e.g., a change from classified sensitive level 3 to classified level 2).

(b) Replacement or modification of the main computer/major system. Not applicable to operation of small computers (e.g., PCs, laptops, notebooks).

(c) A change in the security processing mode to a more complex mode.

(d) A major change to the operating system, or executive software. (Not applicable to operation of small computers.)

(e) A change in the physical environment. Only if the change would introduce new threats and vulnerabilities that would require reassessment under the risk management program.

(f) Any situation that would cause the initial or previously established accreditation to become invalid, for example, newly discovered system insecurities.

(D) **Accreditation Amendment.** When a minor change is made to an accredited AIS, such as the addition of a workstation, an amendment is required. The agency will address a request for an amendment to the ISSM, who will evaluate the request and forward his/her recommendation to the DAA.

(E) **Certifying Official:**

The Certifying Official is usually the organization’s ISSM. The ISSM establishes and administers the organization’s ISSP and is responsible for obtaining accreditation for information systems under the organization’s control. ISSMs are appointed by their commanders, agency chiefs, directorate chiefs, or managers of the activities operating the information system. The Certifying Official will prepare or oversee the preparation of the certification package.

In the case of large or complex systems, the Certifying Official may appoint a Certifying Team to assist with the certification process.

(F) Certification and Accreditation of Networked Systems:

If possible, networks will be certified and accredited as a whole. Any subnet not included in the certification and accreditation (C&A) of the network must be certified and accredited separately.

(G) Interim Accreditation

Normally, all certification tasks must be completed before the Certifying Official requests accreditation from the DAA. However, the DAA may grant interim accreditation when a mission-critical system must be operational before all the required certification tasks are completed. In this case, the Certifying Official must document the residual risks that result from the unfinished certification tasks. The DAA will decide whether he or she is willing to accept the additional risks and AIS Accreditation is defined as the official approval to operate a computer system at a designated level of sensitivity. Formulation of the accreditation documentation is a responsibility of the ISSO. The accreditation process must be completed prior to acquiring a system.

5.2 C&A Documentation Requirements

The following paragraphs explain all of the documentation requirements for HQDA agencies seeking accreditation by IMCEN to operate an AIS within the HEN. Instructions and procedures for preparing an official request for accreditation can be found in the SAM Certification Guide (4). Samples and/or templates for each document required are contained in C&A Package 1 and C&A Package 2 (Reference 6). IMCEN will provide guidance and assistance, as requested, in preparing the accreditation package. IMCEN will provide guidance and assistance, as requested, in preparing the accreditation package.

The requirements for accreditation are intended to be commensurate with the system size, criticality, mode of operation, data sensitivity, and number of users. The accreditation requirements covered in this section are based on the Single Agency Manager (SAM) Certification Guide (Reference 4).

The SAM System Security Requirements Division has established the following policy for IMCEN (5):

(A) Army agencies serviced by IMCEN having no system administrator rights do not need network accreditation.

(B) Army agencies serviced by IMCEN having no ability to manage or administer their computer or network resources or configuration will be accredited as a part of the HQDA Enterprise Network. To be accredited within the HQDA Enterprise Network, HQDA customers must submit the following documents to the IMCEN ISSM:

(1) Certification Request

(2) OISSO Appointment Letter

(3) Configuration Diagram

(4) List and location of hardware and software

(5) Security SOPs Concurrence Memorandum

(6) Information System Security Inbriefing Statement

Samples and templates for each of the above are contained in C&A Package 1 (Reference 6).

(C) Army agencies serviced by the IMCEN having separate external connections or local systems administrators with the ability to manage or administer computer or network resources or configuration will need to provide an independent accreditation package. IMCEN will provide guidance and assistance in preparing the accreditation package for such HQDA customers. They must submit the following documentation to their Certifying Official:

(1) Certification Request

(2) OISSO Appointment Letter

(3) System description, including configuration diagram

(4) Security SOPs or policies, to include a contingency plan

(Guidelines for creating security policies can be found in the SAM Certification Guide [Reference 4]. The IMCEN ISS SOPs may be used as a general guideline.)

(5) Threat Analysis Worksheet

(6) Security Test and Evaluation (ST&E)

(7) Site survey information—if a site survey has been conducted by SAM-DSS.

Samples and templates for each of the above can be obtained in C&A Package 2 (Reference 6), or by contacting IMCEN: Mr. Ronald L. Greenfield, ISSM, 695-7447; or Mr. William Dugger, ISSO, 693-7070.

5.2.1 Sensitivity Determination

(A) Sensitivity determination must be accomplished using the criteria in Section 2.1 and AR 380-19, paragraph 2-2.

(B) When sensitivity has been determined, a written request must be submitted to the DAA for official designation of the sensitivity level that will meet the recommended level. This request accompanies the accreditation request.

(C) Non-sensitive designations must be authorized in the same way as sensitive designations. Each request for non-sensitive designation must be submitted to the DAA for approval and must include the rationale for arriving at this designation. After the operation is officially designated non-sensitive by the DAA, the actual accreditation is not required. However, system operations must be reviewed at 3-year intervals to ensure that the non-sensitive designation remains valid. (Note: only those portions of the accreditation that have changed need to be redone. If no changes have occurred at the end of the 3-year period, an updated accreditation statement from the DAA may be all that that is necessary.)

5.2.2 Interim Approval

(A) A DAA may grant interim approval to operate before an operational accreditation is issued provided the provisions of AR 380-19, paragraph 3-10 are met.

(B) An interim approval may not be granted for periods longer than 90 days and only one additional 90-day extension may be granted.

5.2.3 Accreditation Statement

(A) A system cannot be legally operated without an official accreditation statement on file.

(B) The accreditation statement is signed by the DAA after review of the accreditation documentation. This statement is generated for each accreditation and reaccredidation.

(C) Through this review, the DAA states the highest sensitivity level at which information can be processed, defines the security processing mode, weighs the vulnerabilities and threats against mission requirements, and, by his or her signature, accepts the stated risks for system operation.

6. CONTINGENCY PLAN

6.1 Purpose and Objectives.

(A) The purpose of this contingency plan is to outline a formal plan of action to be followed in the event that the normal IT environment is impaired or disrupted. The impairment or disruption can range from a few hours to several days depending on the cause or situation. This plan consists of a planning, preparation, and action phase and will provide a plan of action for emergency and recovery operations.

(B) The objective of this contingency plan is to provide managers, operations personnel, and users of the computer system with a plan of action. This plan facilitates carrying out required services in a limited fashion and assuring that designated critical and priority jobs can be processed until full recovery can be achieved.

6.2 Scope

The scope and depth of the contingency plan is influenced by the activity's IT environment, the criticality of the functional applications being supported, and the user's IT support requirements. This plan covers the systems in Room's 1B271, 1C616, 1D614, 1D624, 1D629, 1D639, 1D644, 1E600, 1E607, 1E627, 1E629, 1D683, 2E714, 3C635, 3C641, 3C645, 3C711, 3D679 in the Pentagon, and the Warehouse located at 5775 General Washington Dr., Alexandria, VA.

(A) **Limited loss of IT capability.** The impact will vary depending on the urgency or loss potential of individual tasks. Typical causes are as follows:

(1) Failure of key peripheral hardware units or communication circuits

(2) Failure of electric utilities

(3) Loss of key applications programs, preprinted forms, or documentation

(4) Partial loss of air conditioning or power

(5) Non-availability of critical personnel

(6) Sudden expansion in workload due to a national emergency or some other critical event.

(B) **Interruption to IT Operations.** The duration of the interruption will depend on the time needed to restore normal operations. All tasks are usually affected yet with minimal or no damage to the facility. Typical causes are:

(1) Failure of a major computer hardware unit or air conditioning unit

(2) Failure of electric utilities

(3) Fire, flood, or sabotage in the IT operating environment

(4) Intrusion of smoke, dirt, dust, or water

(5) Non-availability of operation personnel

(C) **Major Damage or Destruction of the Facility or Contents.** All operations would be affected. Backup operations and repair of the facility or contents would be required to restore normal operations. Typical causes would be:

(1) Natural acts (earthquake, flood, lightning, etc.)

(2) Civil disorders (bombing, explosions, fire, etc.)

(3) Mechanical breakdown (water pipe bursting, junction box fire)

(4) Catastrophic accidents (airline crash, chemical spills, etc.)

(5) International incident (war)

6.3 Responsibilities

It is the responsibility of the ISSO, the SA, and every individual to understand and follow this contingency plan.

6.4 Situations.

(A) **Personal Injury or Illness:** One of the primary reasons that the “2-persons inside the computer room at all times” regulation is in effect is that if one person becomes disabled in any manner (e.g., accidental electrocution, bad reaction to prescribed medicine, etc.), the other person can administer and/or call for help.

(1) Call for assistance as soon as possible—only life saving and first aid procedures take precedence.

(2) Prevent further injury by removing the person to safety or eliminating hazardous condition, whichever would result in less trauma for the victim.

(3) In the case of electrocution, operate emergency power-off before attempting to touch the victim if they are still in proximity or in contact with the electrical source.

(4) If appropriate, administer CPR, stop arterial bleeding, execute Heimlich maneuver, or other immediate life saving treatment.

(5) Report incident: Call U.S. Army Clinic (695-1031)

(a) Notify FPS - GSA (697-5555)

(b) Notify ISSO – William Dugger (693-7070)

(6) Render assistance to victim(s) until arrival of paramedics:

(a) Make victim(s) as comfortable as possible

(b) Treat for shock

(c) Perform other first aid as appropriate

(B) **Fire within the Room—any rooms described above:**

(1) Report fire (call 697-5555 - notify Pentagon Occupant Emergency Organization Command Center - alternate: Federal Protective Service Operations Office at 697-4151 or GSA Building Manager's Office at 697-7351). Also notify Site Manager.

(2) Activate fire alarm box inside main computer rooms or others in the areas as guides for emergency service personnel to reach the scene.

(3) Assess life-safety hazard; evacuate facility if necessary.

(4) Initiate loss control procedures:

(a) Time permitting, secure classified processing.

(b) If fire involves electric power source/cable, use emergency power-off.

(c) If fire involves localized support equipment, terminate power to unit if possible, power down system gracefully. Extinguish fire in the equipment if possible.

(d) If fire involves documents, printer paper, and/or magnetic storage media or other concentrations of combustible material, attack fire as soon as practicable; power down system gradually following apparent extinguishment; check material for re-ignition.

(5) Assist fire department firefighters upon arrival.

(6) Re-secure facility following completion of emergency service activity.

(C) **Evacuation Due to Fire Elsewhere in Pentagon:**

(1) Notify ISSO/Site Manager.

(2) Shut down system gracefully.

(3) Time permitting, secure classified material.

(4) Lock doors upon departure.

(5) Proceed to appropriate marshalling area via safest route.

(D) **Evacuation Due to Hazardous Chemical Spill:**

(1) Notify ISSO/Site Manager.

(2) Shut down system(s) gracefully.

(3) Time permitting, secure classified material.

(4) Lock doors upon departure.

(5) Proceed to appropriate marshalling area via safest route.

(E) **Evacuation Due to Bomb Threat:**

(1) Notify ISSO/Site Manager.

(2) Shut down system(s) gracefully.

(3) Time permitting, secure classified material.

(4) Lock doors upon departure.

(5) Proceed to appropriate marshalling area via safest route.

(F) **Evacuation Due to Rioting/Terrorist Actions on Pentagon Grounds:**

(1) Notify ISSO/Site Manager.

(2) Shut down system(s) gracefully.

(3) Time permitting, secure/destroy classified material (see Section 2.3)

(4) Lock doors upon departure.

(5) Proceed to appropriate marshalling area via safest route.

(G) **System Crash:**

(1) Evaluate console message(s).

(2) Isolate component(s) to minimize system disruption.

(3) Examine components to determine whether any damage occurred.

(4) Notify ISSO of system status and anticipated actions.

(5) Tag affected component(s) and log details of incident to facilitate subsequent corrective action.

(6) Download active files to secondary storage prior to system shutdown; be especially aware of securing classified data.

(7) ISSO will do the following:

(a) If system is still up, message to alert system users to specific degradation problem.

(b) Dispatch personnel to assist operator(s) in troubleshooting and restoring system, if possible.

(c) Contact appropriate entity to request necessary repairs (i.e., vendor’s customer/field engineer, lead systems programmer, hardware technician, etc.).

(d) Post message to system users.

(H) **Equipment Damage:**

(1) If needed, effect life safety measures immediately.

(2) Isolate and shut down unit(s) affected.

(3) Report condition to ISSO/Site Manager.

(4) Evaluate effect on system operation and take actions to minimize disruption.

(5) Locate articles that are evidence of equipment failure and establish safeguards to prevent their disturbance prior to investigation.

(I) **Unscheduled Power Outage, Surge, or Other Electrical Irregularity:**

(1) Following a system crash, inspect equipment for damage. If needed, request a thorough inspection and test by vendor Customer/Field Engineer(s) prior to restoring system on-line.

(2) When system remains on-line following a power fluctuation which contaminates the operating system or applications, bring the system down gracefully and perform a standard restart and recovery operation, paying particular attention to the classified side of the system.

Note: *When there is a potential for local extreme thunderstorm activity, systems should be shut down to prevent damage likely to result from power surges and blackouts as well as electromagnetic interference with transmission lines from lightning discharges. Systems shall be brought down gracefully prior to scheduled power outages.*

(J) **Smoke or Excessive Dust in Main Computer Rooms:**

(1) Notify ISSO/Site Manager.

(2) Shut down all equipment gracefully.

(3) Seal all IT media, including classified, in appropriate containers or remove from room.

(4) Seal door(s) edges with tape upon departure if possible and activate locks.

(5) Evacuate area when necessary.

(K) **Excessive Heat/Humidity within Main Computer Rooms:**

(1) Notify ISSO/Site Manager.

(2) Check HVAC (heating, ventilating, air conditioning) operations

(a) Air handling unit re-circulating fan running?

(b) Chill water temperatures satisfactory?

(c) Filters satisfactory?

(3) Check adjacent areas to determine if room temperatures outside the computer rooms are also excessive.

(4) When directed, shut down peripheral equipment to reduce heat load; also turn off fluorescent lighting if possible. (Temperature in excess of 80 degrees F or relative humidity greater than 65%.)

(5) Set up pedestal fan(s) to help cool CPU/disk drive cabinets

(6) Notify users to terminate sessions when temperature exceeds 83 degrees F.

(7) Shut down CPU and disk drives when temperature exceeds 85 degrees F or relative humidity exceeds 80%, making certain to secure classified processing.

(8) Have vendor’s Customer/Field Engineers) examine and test IT equipment prior to restoring normal system use

(9) ISSO/Site Manager:

(a) Initiate trouble call to the GSA Pentagon Building Administrator (695-270).

(b) Contact Utility Systems Repair Operator (697-7351) to ascertain the status of climate control conditions for the sector(s) affected.

(c) If the prognosis for conditions in the immediate area surrounding computer room indicates continuing degraded climate control, instruct operator(s) to phase out peripheral and processing equipment, thereby minimizing potential damage.

(L) **Insufficient Heat/Humidity within Main Computer Room:**

(1) Check air handling unit for satisfactory operation.

(2) Notify ISSO/Site Manager when temperature drops below 65 degrees F, humidity drops below 45% or if static electricity is evident.

(3) If temperature continues to drop and adjacent rooms also exhibit insufficient heating during winter conditions, request instruction from ISSO.

(4) ISSO/Site Manager:

(a) Contact Utility System repair operator (697-7351) to ascertain the status of building climate control for the sector(s) affected.

(b) Initiate trouble call to restore local utility operation.

(c) Order system shut down when building conditions are expected to continue degrading as a result of utility failure.

Note: *Disk/tape drive misalignment is to be expected for read/write operations occurring at widely divergent temperatures--subsequent attempts to recover data are not likely to be successful unless performed under similar conditions.*

(M) **Water Damage in Computer Room:**

(1) Notify ISSO.

(2) Shut off source of leak, if possible.

(3) Terminate jobs in progress after posting a system warning message to users to conclude processing.

(4) Spin down and remove disk(s) from drive(s).

(5) Power down hardware and cover with plastic sheeting.

(6) Power down air conditioning equipment.

(7) Put tapes, disks, run books, and source documents in storage container(s) or remove from site.

(8) Stand by to provide access for utility repair crew. (Secure space when unattended.)

(9) Site Manager:

(a) Assess extent of service interruption (repair operations may result in loss of air conditioning for an extended period--significant moisture within the computer room may necessitate comprehensive computer system inspection and testing prior to restoring on-line service).

(b) Submit trouble call to Utility Systems Repair Operator (697-7351 or 695-7622).

(10) ISSO: Post message(s) to affected system(s) to advise users of conditions and of the probably duration of the outage.

(N) **System Overload Due to Heavy Usage:**

(1) Short Term Prognosis (less than 36 hours):

(a) ISSO:

(i) Notify user agency Functional Manager(s) of the overload condition and recommend that users be instructed to purge their unnecessary files.

(ii) Post system message(s) apprising of degradation and requesting reduction of unnecessary usage.

(iii) Selectively download inactive files to backup pending archival requests.

(b) Site Manager:

(i) Query users as to the status of their activity.

(ii) Designate users, files, and applications, which can be withdrawn from on-line use temporarily to alleviate the excess usage.

(iii) Review procedures in use to effectively purge outdated information from the system and to archive documents needed for subsequent retrieval.

(2) Long Term Prognosis (in excess of 36 hours)

(a) Site Manager: Convene planning group to assess:

(i) The prevailing conditions

(ii) The likelihood of a need for specific additional resources

(iii) The potential for satisfying the projected requirements without disrupting routine business.

(O) **System Overload Due to Conflicting User Requirements:**

(1) Short Term Prognosis

(a) ISSO:

(i) Notify user agency Functional Manager(s) of the overload condition and recommend that users be instructed to purge their unnecessary files.

(ii) Post system message(s) apprising of degradation and requesting reduction of unnecessary usage.

(iii) Selectively download inactive files to backup pending archival requests.

(b) Site Manager:

(i) Query users as to the status of their activity.

(ii) Designate users, files, and applications, which can be withdrawn from on-line use temporarily to alleviate the excess usage.

(iii) Review procedures in use to effectively purge outdated information from the system and to archive documents needed for subsequent retrieval.

(2) Long Term Prognosis (in excess of 36 hours)

(a) Site Manager: Convene planning group to assess:

(i) The prevailing conditions

(ii) The likelihood of a need for specific additional resources

(iii) The potential for satisfying the projected requirements without disrupting routine business.

(P) **Physical Intrusion by Unauthorized Personnel:**

(1) Notify Site Manager; providing enough detail to allow for adequate response.

(2) Advise intruder(s) of restricted status of space and ask intruder(s) to leave.

(3) Prepare to shut down system if potential for damage or compromise of classified data is indicated.

(4) If weapons are carried by intruder(s), do nothing to antagonize, but cooperate to the extent that system resources are not hazarded. Comply with demands if life safety is threatened.

(5) Note characteristics of intruder(s) to facilitate reporting after the incident.

(6) Assist Pentagon security personnel upon their arrival.

(Q) **Unauthorized System Access Attempt:**

(1) ISSO:

(a) Periodically, review Sun system audit trial to determine if any sources of impropriety exist. If found, request interception and notification of file owner.

(b) Initiate interactive system countermeasures to isolate activity of penetrator.

(R) **Discovery of Physical Resource Tampering:**

(1) Notify ISSO.

(2) Preserve evidence for subsequent investigations.

(3) Note conditions at the time of discovery.

(4) Prevent access by all personnel not directly involved with resolution of the incident.

(5) ISSO:

(a) Dispatch functional supervisor to the scene.

(b) Request investigative support of site and/or advisement of INSCOM/ACSI as necessary.

(c) Advice person(s) on scene of anticipated actions by respondents.

(S) **Discovery of Software Resource Tampering:**

(1) Notify ISSO.

(2) Preserve evidence for subsequent investigations.

(3) Note conditions as to how discovered, etc.

(4) Prevent access by all personnel not directly involved with resolution of the incident.

(5) ISSO:

(a) Dispatch functional supervisor to the scene.

(b) Request investigative support of site and/or advisement of INSCOM/ACSI as necessary.

(c) Advice person(s) on scene of anticipated actions by respondents.

(T) If the MMAC Plus hub fails or malfunctions in a way that affects the performance of the HQDA/FDDI Network:

(1) Call Cabletron for maintenance on the switch. IMCEN has full maintenance on the MMAC Plus chassis, environmental module, power supplies, and all cards except the Ethernet cards. IMCEN does not maintain spare Ethernet cards. The Cabletron POC to be notified is either Mark S. Willis (697-2965).

(2) The UPSs that the MMAC Plus is connected to should keep the MMAC Plus switch up for at least one hour.

Appendix A References

1. AR 380-5, *Information Security Program*, 25 February 88.
2. AR 380-19, *Information Systems Security*, 1 August 90.
3. *Pentagon Automated Information System (AIS) Security Manual*, Single Agency Manager, July 1998.
4. *Single Agency Manager (Sam) Certification Guide*, Single Agency Manager, 22 July 1998.
5. *Security Certification of the HQDA Enterprise Network*, Single Agency Manager (SAM) System Security Requirements Division Memorandum, May 1999.
6. *Templates for Certification and Accreditation to Operate within the HQDA Enterprise Network* and *Templates for full Certification and Accreditation to Operate within the HQDA Enterprise Network*, prepared by IMCEN, September 1999.
7. Draft *HQDA Information Systems Security Reference Manual*, Version 1.3, March 1999.
8. *Information Systems Security Management Business Process Analysis Report*, Version 1.2, Federal Systems Integration and Management Center, prepared for HQDA IMCEN, September 1998.
9. Public Law 100-235, “Computer Security Act of 1987,” 8 January 1988.
10. DOD 5200.1: *DOD Information Security Program*, 13 December 1996.
11. Letter of Instruction (LOI) #1-99: *HQDA Email Site Policies and Guidelines*, from JDIM-ZA, 23 June 1999.
12. *Administrator Account Controls and Procedures*, HQDA ARDA SOP 98-09, 15 July 1998
13. DOD 8220.1: *Single Agency Manager Directorate of Security (SAM-DS) for Pentagon Information Technology Services (ITS)*, 1 March 1995.
14. DISA Instruction 630-230-19: *Information Systems*, *Information Systems Security*.
15. *Interim Operational Security Doctrine for SBU Fortezza Cards*, NAG 69-B, 241619Z, February 1998.
16. *Defense Message System Operating Policies and Procedures*, DISAC 310-70-xxx (Draft), February 1998.
17. *Physical and Operational Security of the Certification Authority Workstation (CAW,)* Single Agency Manager Pentagon Telecommunications Service Center Operating Instruction 31-11, 13 March 1998.
18. Memorandum, Subject: Chief Information Officer Instruction—Army Messaging Standards for Microsoft Exchange (AMSME), SAIS-PAA-S, 13 May 1999.

Appendix B X.509 Certificate Request Form

The following page contains a sample of the X.509 Certificate Request Form. Do not complete this form on line, i.e., electronically. Print it out and complete it separately in hard copy.

X.509 CERTIFICATE REQUEST FORM

Tracking #_________
(FOR CA USE ONLY)

User Information

1. Action Type ______________________________

2. Recipient Name ______________________________
(Last, First, MI, Grade/Title)

Phone
Comm:____________________
DSN:____________________

3. Recipient Address (*for delivery of Fortezza card*)
UNIT:______________________________
STREET:______________________________
CITY/APO/FPO:______________________________
STATE:

4. PIN Address (*for delivery of PIN letter; must be different from block 3*)
UNIT:______________________________
STREET:______________________________
CITY/APO/FPO:______________________________
STATE:

5. Recipient Email Address: □ **SMTP**

6. Recipient Signature **Date:**

Certificate Information

7. Certificate Type (*Select only one*)
□ INDIVIDUAL
□ ORG. FIRSTBORN
□ ORG. SIBLING

8. Certificate Classification: (*Select only one*)
□ TOP SECRET
□ SECRET/CONFIDENTIAL
□ SENSITIVE BUT UNCLASSIFIED

9. Precedence Privileges: (*Only for Organizational Certificates)*)
□ CRITIC/FLASH
□ IMMEDIATE PRIORITY
□ ROUTINE/DEFERRED

10. Send/Receive Privileges: (*Only for Organizational Certificates)*)
□ ORG. RELEASE AUTHORITY
□ READ ONLY

11. Comments (See instructions; continue on separate sheet if necessary):
____
____
____

12. Certificate Validity Period: 156 *weeks*

13. Personality Name:______________________________

Administrative/Signature Block

14. Card Chip Serial Numbers
____
____
____

15. Type of Identification:
____
____
____

16. DISTINGUISHED NAME
____
____

17. Supervisor Name *(print)* **Comm:**____________
______________________________**DSN:**____________
(Last, First, MI)
________________________/__________
Signature/Date

18. Sub-Registration Authority Name *(print)* **Comm:**____________
______________________________**DSN:**____________
(Last, First, MI)
________________________/__________
Signature/Date

19. Org. Registration Authority Name *(print)* **Comm:**____________
______________________________**DSN:**____________
(Last, First, MI)
________________________/__________
Signature/Date

20. Certification Authority Name *(print)* **Comm:**____________
______________________________**DSN:**____________
(Last, First, MI)
________________________/__________
Signature/Date

Appendix C Instructions for Completing the X.509 Certificate Request Form

TRACKING NUMBER

The Tracking Number will be assigned when the Certification Authority (CA) receives the X.509 Certificate Request Form. This blocked is reserved for the Certification Authority only.

USER INFORMATION

(To be completed by the user)

BLOCK 1 (ACTION TYPE)

Enter an action to be performed. Some actions require an explanation in Block 11 by the end user or Organization Registration Authority (ORA). Following each action description below is a list of X.509 Request Form block numbers. The corresponding blocks should be completed if that action type is selected. Types of actions include the following:

1. CHANGE PIN. This allows the CA to change the user PIN on a FORTEZZA card that they created. Complete the following blocks: 1, 2, 3-4 (if mailed), 6, 11, 17.
2. CHANGE USER INFORMATION. This action results in modifications to the User Database (name, address, etc.). These changes do not affect the certificate. Complete the following blocks: 1-6.
3. COMPROMISE REPORT. When a card has been compromised (lost, stolen, etc.), the Keying Material Identifier (KMID) must be reported to the CA as soon as possible (within 24 hours). Complete the following blocks: 1, 2, 6, 11 (brief description i.e. lost, stolen, etc.), 13, 14,17. Attach a detailed report in accordance with NAGs 66 and 68.
4. COPY CARD. This action results in a card with is a duplicate copy of the original card, but with a different PIN. Complete the following blocks: 1, 2, 3-4 (if mailed), 6, 11, 17.
5. DELETE PERSONALITY. This allows the CA to delete a personality (certificate) from the FORTEZZA card that the CA has created. Complete the following blocks: 1, 2, 3-4 (if mailed), 5, 6, 10, 11, 13, 17.
6. NEW CERTIFICATE. Requests a new X.509 certificate for the individual, equipment or organization. This includes to change the Distinguished Name (DN) on an existing certificate. Complete the following blocks: 1, 2, 3-4 (if mailed), 5-9, 12, 13, 17.
7. RENEW. This action extends the validity period of an existing X.509 certificate. Complete the following blocks: 1, 2, 3-4 (if mailed), 5, 6, 12, 13, 17.
8. REKEY. This action replaces a Digital Signature Standard (DSS) and/or Key Encryption Algorithm (KEA) with a new key. The attributes for this new certificate are

identical to those of the original X.509 certificate that is being re-keyed. Specify the key (Digital Signature Standard or Key Encryption Algorithm or both) which is to be re-keyed. Complete the following blocks: 1, 2, 3-4 (if mailed), 5, 6, 11, 13, 17.

9. RESTORE. This action will restore the certificate(s) created by a Certification Authority to the card. Indicate in Block 11 the personality name or Distinguished Name of the certificate to be restored, or the card chip, serial number if an entire card is to be restored. Complete the following blocks: 1, 2, 3-4 (if mailed), 5, 6, 11, 13, 17.

10. REVOKE CERTIFICATE. This action will revoke a certificate in the Certification Authorities database, for placement on a Certificate Revocation List (CRL). Complete the following blocks: 1, 2, 6, 11, 13, 16, and 17.

11. UPDATE CERTIFICATE. This action will modify the certificate attributes (clearance levels or privileges). The original certificate is revoked, but the Distinguished Name is retained. Complete the following blocks: 1, 2, 3-4 (if mailed), 5, 6, 7-10 (as applicable), 11, 13, 16, 17.

BLOCK 2 (RECIPIENT NAME)

Print the name and grade/title of the person who will be responsible for the card. This person is the recipient or end user of the card and will use it to perform their duties. Enter the commercial and/or DSN telephone numbers (if applicable) of the user.

BLOCK 3 (RECIPIENT ADDRESS)

This is where the FORTEZZA card will be shipped.

1. HAND DELIVERY. If hand delivery is the means of delivery, then enter the room number where the user’s ORA is located.

2. REGISTERED MAIL. If registered mail is the means of delivery, then enter unit address.

BLOCK 4 (PIN ADDRESS)

This is where the FORTEZZA PIN letter will be shipped.

1. HAND DELIVERY. If hand delivery is the means of delivery, then enter the room number where the user is located.

2. REGISTERED MAIL. If registered mail is the means of delivery, then enter the user’s home address. This address must be different from the Recipient Address (block 3).

BLOCK 5 (RECIPIENT E-MAIL ADDRESS)

Enter the e-mail address that the Certification Authority can use to transmit official communications that pertain to the FORTEZZA cards and certificates (i.e. notification for re-keying of material on the FORTEZZA card, updated CRLs, ext.).

BLOCK 6 (RECIPIENT SIGNATURE)

The person listed in block 2 must sign and date this form prior to submission.

CERTIFICATE INFORMATION

(To be completed by the supervisor and Organization Registration Authority)

BLOCK 7 (CERTIFICATE TYPE)

Enter the type of certificate to be generated for the user. The following is a list of the types of certificates to be used by the users:

1. INDIVIDUAL. This certificate will be used by an individual person rather than by an organization.
2. ORGANIZATIONAL FIRSTBORN. This certificate is the first to be requested on behalf of a specific organization; subsequent requests shall be marked as Organizational Siblings (see below). The organizational firstborn certificate contains the Key Encryption Algorithm that will be shared by the organization.
3. ORGANIZATIONAL SIBLING. This certificate will be used on behalf of an organization and it shares the Key Encryption Algorithm, inherits the certificate classification and precedence privileges of the Organizational Firstborn.

BLOCK 8 (CERTIFICATE CLASSIFICATION)

This is the classification of the certificate, for which the user can send and/or read messages (this is not the actual security clearance of the end user). Place an X in the block that applies.

BLOCK 9 (PRECEDENCE PRIVILEGES)

This is the precedence that the user may send messages. The following is a list based on the type of certificate being issued:

1. INDIVIDUAL. For individual certificates, Routine/Deferred is the only privilege allowed for individual messaging.
2. ORGANIZATIONAL FIRSTBORN. For organizational firstborn certificates, any or all the privileges maybe selected, but remember the organizational sibling certificate will inherit those same privileges.
3. ORGANIZATIONAL SIBLING. For organizational sibling certificates there is no need to select the precedence because the sibling inherits these privileges from the firstborn.

BLOCK 10 (SEND/RECEIVE PRIVILEGES)

This field is for Organizational Certificates only. This allows the user to either digitally sign messages, encrypt messages with the Key Encryption Key (KEK) or both. The organizational release authority allows the user to digitally sign and encrypt messages with the Key Encryption Key. The read only allows the user to read organizational mail, but not send on the behalf of the organization through digital signature.   The digital signature is what allows the user to send on behalf of the organization. Place an X in the blocks that apply.

BLOCK 11 (COMMENTS)

A written explanation/justification is required for the following actions (refer to block 1 of the instructions):

1. COMPROMISE REPORT. Fill in the affected Keying Material Identifier(s) (if known) and reason for compromise.

2. NEW CERTIFICATE. If this is a new certificate on an existing card, indicate the card chip serial number from the card label.

3. COPY CARD. Indicate the reason for the copy card request (i.e. traveling user, card to be used outside of a classified enclave, or support equipment, etc.).

4. ORGANIZATIONAL SIBLING. Indicate the serial number or the Distinguished Name of the Firstborn Organizational Certificate.

5. REKEY. Indicate which key (Digital Signature Standard, Key Encryption Algorithm, or both) must be re-keyed.

6. RESTORE. State why the card or certificate needs to be restored.

7. REVOKE CERTIFICATE. State the reason why the certificate needs to be revoked prior to its normal expiration date.

BLOCK 12 (CERTIFICATE VALIDITY PERIOD)

The validity period for the certificate is three years (156 weeks).

BLOCK 13 (PERSONALITY NAME)

Enter the name that the individual will use to identify a certificate on the FORTEZZA card. The Organization Registration Authority will need to provide the name for this block to avoid duplicate names.

ADMINISTRATIVE/SIGNATURE BLOCK

This section is for administrative information and the approval signatures. Block 14; will be, completed by the Certification Authority. Block 15; will be, completed by the Organization Registration Authority. Block 16; will be, completed by the Sub-Registration Authority.

BLOCK 14 (CARD CHIP SERIAL NUMBER)

This is the internal chip serial number for the FORTEZZA card. The card serial number is found on the label of the card. This number is also referred to as a Keying Material Identifier.

BLOCK 15 (TYPE OF IDENTIFICATION)

The type of identification that is used to verify the recipient's identity.

BLOCK 16 (DISTINGUISHED NAME)

The Distinguished Name is obtained from the Sub-Registration Authority for the recipient's certificate.

BLOCK 17 (SUPERVISOR NAME)

Print the name of the supervisor who is approving the requested action. Enter the commercial and DSN telephone number(s) of the supervisor. Obtain the supervisor's signature when the form is ready for submission. Before signing, the supervisor should verify blocks 7-12.

BLOCK 18 (ORGANIZATIONAL REGISTRATION AUTHORITY NAME)

Print the name of the Organization Registration Authority who verifies the information on the form (NOTE: The Organization Registration Authority is responsible for the verification of the user's security clearance through the Organization's Security Officer). Enter the commercial and DSN telephone number(s) of the Organization Registration Authority. Obtain the Organization Registration Authority's signature when the form is ready for submission.

BLOCK 19 (SUB-REGISTRATION AUTHORITY NAME)

Print the name of the Sub-Registration Authority who enters the Distinguished Name (block 16). Enter the commercial and DSN telephone number(s) of the Sub-Registration Authority. Obtain the Sub-Registration Authority's signature once the Distinguished Name has been placed on the X.509 Request Form.

BLOCK 20 (CERTIFICATION AUTHORITY NAME)

The Certification Authority who is completing the request will print his/her name, and complete the form.

Appendix D Organizational Registration Authority (ORA) Appointment Memorandum

On the following page is the memorandum template for use in appointing an Organizational Registration Authority (ORA). The ORA is the administrative authority that registers end-users of Fortezza cards with the Single Agency Manager (SAM) Certification Authority (CA). Responsibilities of the ORA are detailed in Section 2.8 of these SOPs. The Director of the agency/organization, or whomever he delegates this authority to, will appoint the primary ORA and any alternates on orders and will complete and forward the ORA Appointment Memorandum to the agencies shown in the distribution list.

MEMORANDUM

To: [SEE DISTRIBUTION]

From: [Click **here** and type name]

Subject: Additional Duty Assignment

Date: 01/12/00

Effective [DATE HERE], the individual listed below is appointed as Defense Message System Organizational Registration Authority (ORA) for the DATE HERE[ORGANIZATION HERE]

Name: [First, Last, MI), Rank]

Unit Address:

AUTHORITY: AR 25-reg (Draft 3), Defense Message System Registration Hierarchy and Directory Services and Registration Basic Policies and Procedures, Paragraph 6-7, June 1998.

PURPOSE: To gather and verify information about a select group of DMS users.

PERIOD: Until officially released from appointment or assignment.

SPECIAL INSTRUCTIONS: None.

[Appointing Officials Name]

[Organization]

DISTRIBUTION:

(1) HQDA DMS Sub-Registration Authority

(1) HQDA Certificate Authority

(1) Individual

Appendix E Glossary

This glossary provides definitions of acronyms and key terms used in this document. For a more comprehensive listing of terms, see the *Pentagon AIS Security Manual*, which is separately maintained and available through the IMCEN ISSM or directly from the Single Agency Manager.

ACRONYMS

AA	Administrative Assistant to the Secretary of the Army
AIS	Automated Information System
AISSP	Automated Information System Security Plan
AR	Army Regulation
ARDA	Army, Department of Army
CA	Certificate Authority
C&A	Certification and Accreditation
CONOPS	Concept of Operations
DAA	Designated Approving Authority
DMS	Defense Message System
DOD	Department of Defense
DOIM	Director of Information Management
FOA	Field Operating Agency
FOUO	FOR OFFICIAL USE ONLY
FW&A	Fraud, Waste, and Abuse
HEN	HQDA Enterprise Network
HQDA	Headquarters, Department of the Army
ICCC	IMCEN Configuration Control Committee
IMCEN	Information Management Support Center
IMO	Information Management Office
IP	Internet Protocol
ISS	Information Systems Security
ISSM	Information Systems Security Manager

ACRONYMS

ISSMP	Information Systems Security Management Program
ISSO	Information Systems Security Officer
ISSP	Information Systems Security Program
ISSPM	Information Systems Security Program Manager
ISSRM	Information Systems Security Reference Manual
ITS	Information Technology Services
LAN	Local area network
LOI	Letter of Instruction
ODISC4	Office of Director of Information Systems - Command, Control, Communications, and Computers
OISSO	Organization Information Systems Security Officer
ORA	Organizational Registration Authority
OSD	Office of the Secretary of Defense
PC	Personal computer
PIN	Personal identification number
POC	Point of Contact
SA	System Administrator (SA)
SAP	Special Access Program
SBU	Sensitive but Unclassified
SCI	Sensitive Compartmented Information
SLOP-ESI	Single Integrated Operational Plan Extremely Sensitive Information
TASO	Terminal Area Security Officer
UPS	Uninterruptible Power Supply
WAN	Wide area network

DEFINITIONS

Accreditation A formal declaration by the DAA that an AIS is approved to operate in a particular security mode using a prescribed set of safeguards.

Certification The comprehensive evaluation of the technical and non-technical security features of an Automated Information System (AIS) and other safeguards, made in support of the accreditation process, to establish the extent to which a particular design and implementation meets a specified set of security requirements.

Incident Response and Reporting The proper reporting and disposition of security incidents to assess and mitigate damage associated with poor user procedures and system vulnerabilities.

Malicious Logic Code designed with a malicious intent to deny, destroy, modify, or impede systems configuration, programs, data files, or routines. This code is generally termed a “virus.”

Network Security Protection of networks and their services from unauthorized modification, destruction, or disclosure, and provision of assurance that the network performs its critical functions correctly and that there are no harmful side effects.

Security Policy Establishment of responsibilities and procedures to support the Pentagon AIS security program. SAM-DS security policy is promulgated in the Pentagon AIS Security Manual (see Section 1.6 References).

Security Program Review A newly developed SAM program whose mission is to evaluate and assess customer ISSP and to provide feedback on the customer’s level of satisfaction with SAM-DS security services.

Training and Education A security education and awareness program for all Pentagon IS users, including ISSMs, ISSOs, OISSOs, SAs, and end users.

Fortezza Card A personal computer card that uses approved algorithms and procedures to provide network related security services.